Albrecht Weinert

Windows 2003 Domain

Migration von NT4 mit Fremd-DNS

Prof. Dr.-Ing. Albrecht Weinert

Labor für Medien und verteilte Anwendungen (*MEVA*-Lab)

Fachbereich 3 Elektrotechnik und Informatik
Fachhochschule Bochum

Dokument: W2K3Domain1p.doc (Vorlage NUTZ.DOT), erstellt am 16. August 2005

Version	**Datum**	**Autor**	**Änderung / Anlass**
V 0 . 0	17.08.2005	Weinert	neu
V 0 . 1	19.08.2005	Weinert	Stand “Schritt A) abgeschlossen” (s. Kap. 1.4, Seite 5)
V 0 . 3	05.09.2005	Weinert	Ergänzungen zu A); Stichworte zu B)
V 0 . 3	13.09.2005	Weinert	Beginn der Beschreibung “PC-Labor...”
V 0 . 4	21.09.2005	Weinert	Nutzerstruktur und (40) Schulungsrechner
V 0 . 5	28.09.2005	Weinert	“operabler” Zwischenstand “beta2”
V 1 . 0	04.10.2005	Weinert	Zustand Semesterstart (~1300 Nutzerkonten)
V 1 . 1	26.10.2005	Weinert	Finetuning, Beginn Automat.v..Admin., Korr. Erste Erfahr.
V 1 . 2	14.01.2006	Weinert	FH-Druckdienst (Beginn)

Letzte Änderung am 14.01.06, 16:45 (letztes Speicherdatum)

Vorwort

Die Migration einer NT4-Domäne nach Windows Server2003 (als DC) ist ein von Microsoft gut unterstützter Vorgang. Komplizierter wird es eigentlich erst, wenn Nebenbedingungen in einem heterogenen Firmennetz hinzukommen. Dies gilt insbesondere dann, wenn dies das (Firmen-) DNS und -DHCP sowie -LDAP und AD betreffen.

Hinweis: Alle verwendeten Abkürzungen finden Sie im Anhang 5.3 ab Seite 32.

Für die Domäne FB3-MEVA des Labors für Medien und verteilte Anwendungen (*MEVA*-Lab) im Fachbereich Elektrotechnik und Informatik (FB3) der Fachhochschule Bochum stand solch eine Migration von NT4 nach W2K3 an. Hierbei galten und gelten die oben angedeuteten komplizierenden Nebenbedingungen eines homogenen und fremdgesteuerten Firmennetzes. Im Rahmen der Migration sollte zudem noch eine heterogene (Multi-) Domain-Struktur aus NT4- und Linux-Domänen zu einer W2K3-Domäne konsolidiert werden.

Für die weitere Betreuung und Administrierung der so konsolidierten *MEVA*-Lab-IT-Infrastruktur ist eine ausführliche Dokumentation der Vorgänge und Verfahren unerlässlich.

Das Vorliegende ist zum Einen ein Teil dieser (internen) Dokumentation. Zum Anderen mag es als Erfahrungsbericht aber auch Anderen in ähnlicher Lage hilfreich sein. In diesem Sinne ist auch die Ausgangslage etwas ausführlicher geschildert, als es die Dokumentation des neuen Zustands allein erfordert hätte.

Im Sinne der (speziellen) *MEVA*-Lab-Dokumentation, also der ersten Rolle, werden in Folgenden einfach die konkreten Rechnernamen, i.A. in der Form PD3xyz genannt. Im Sinne eines allgemeingültigen Erfahrungsberichts für andere Anwender sind dies natürlich nur Platzhalter im Sinne von DC1, WS1 und Ähnlichem. Die Tabelle 3 auf Seite 10 und das Kapitel 1.2, Seite 4, helfen beim „Übersetzen“.

Inhaltsverzeichnis

1 Ausgangslage

Bild 1: Das Logo des Labors für Medien und verteilte Anwendungen — *MEVA*-Lab (als Aquarell, 62 * 45 cm^2, Albrecht Weinert, 2001)

Die Darstellung von Diensten und Anwendungen, auch ja insbesondere solchen mit harten Echtzeitanforderungen, in einer vernetzten Umgebung ist das Arbeitsgebiet des Labors für Medien und verteilte Anwendungen, kurz *MEVA*-Lab. Dies Ziel wird auch im Logo des Labors, Bild 1 und rechts, symbolisiert.

Zur Darstellung von IT-Diensten für die Labore und den Fachbereich Informatik ist die Domäne FB3-MEVA ein wesentliches Mittel.

1.1 Dienste

Die Domäne FB3-MEVA erbringt zahlreiche Dienste für das aus den Laboren AT-Labor, MaC-Lab und *MEVA*-Lab bestehende Institut für IT-automation sowie auch für den Fachbereich Elektrotechnik und Informatik (FB3) der Fachhochschule Bochum.

Diese Dienste sind u.A.

- Konten für alle FB3-Kolleginnen und Kollegen
- Konten für alle Büro- und Laborrechner des Instituts (ca. 30)
- Druckservice
- File-Service
- Backup
- Versionsverwaltung mit CVS und Subversion (SVN-Server)
- Objektschutz für Labore und Büros in den D-Gebäuden des Fachbereichs 3
- WWW-publishing für den FB 3

Hinzu kamen bis 2002

- Benutzerkonten für Studierendengruppen (wie java, cax u.dgl.)
- Benutzerkonten für einige Studierende mit Sonderrollen (wie Hilfskräfte und Diplomanden)
- Konten für ca. 40 Laborrechner im studentischen Schulungsraum (CAX-Labor).

Diese Konten und zugehörigen Dienste wurden, wie in Kapitel 1.3 auf Seite 5 geschildert, im Jahr 2002 erweitert und in eine getrennte Linux-Domain ausgelagert.

1.2 FB3-MEVA - Server

Die erwähnten Dienste (u.A.m.) wurden in der Domäne FB3-MEVA von einigen Servern erbracht. Im Zustand der Ausgangslage (Juli 2005) waren dies:

- Rechnername BeSy, Funktion
- PD321S NT4 PDC
- PD322S NT4 BDC
- PD323S NT4 BDC
- PD313D W2K3 SrvStd Druckserver
- PD3082 W2K3 SrvEnt Backup, Version
- PD310S W2K3 SrvEnt WWW-publish (Wichtel)
- PD3082 W2K3 SrvEnt Backup, Version

Hinzu kommen einige wesentliche Workstations (Stand Juli 2005):

- PD3091 W2K WS Objektschutz (Wächter)
- PD309S W2K3 SrvStd Eisenbahn (Projekt)
- PD302x W2K WS div. Bürorechner
- PD30xL W2K WS div. mobile Rechner
- PD3084 W2K WS Grafik-Workstation (Scanner, Photo)
- PD308D W2K WS Dozentenrechner, auch für Beamer und Funk-Tastatur und -Maus für einen Seminarraum (D3-12)
- PD3xyz W2K WS div. Workstations für Studierende und Diplomanden

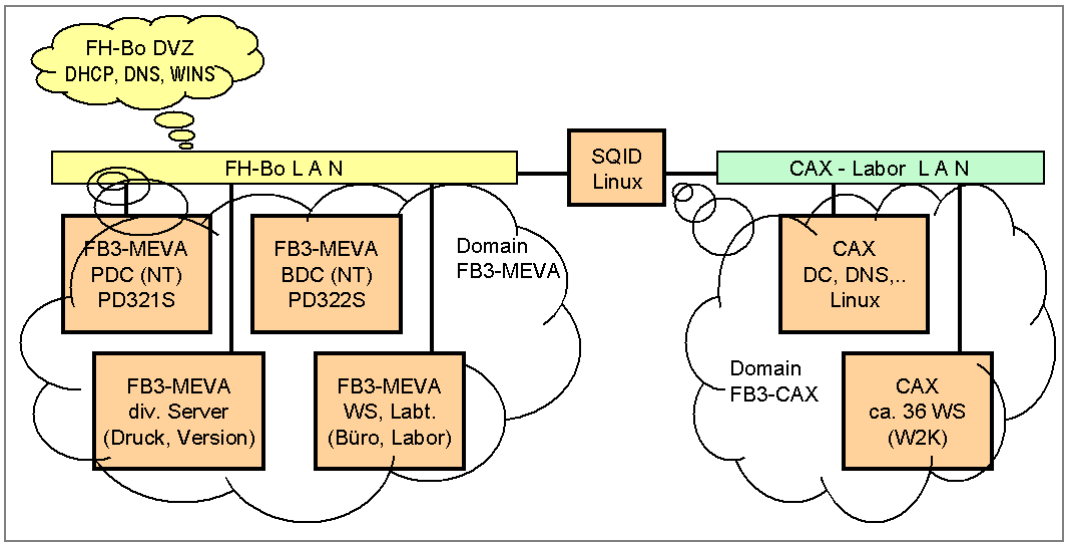

Bild 2: Die Ausgangslage, Domänenstruktur FB3-MEVA und Schulung (CAX)

1.3 Domain-Aufbau bis Juli 2005

Die Domäne FB3-MEVA war bis Juli 2005 eine NT4-Domain. Die Rechner, die Server und auch die DCs sind an das LAN der FH Bochum angeschlossen und bedienen sich der dort gebotenen Infrastruktur. Das heißt in diesem Zusammenhang vor Allem DNS, WINS und DHCP. Insbesondere wurde in der (NT-) Domain FB3-MEVA keiner dieser Dienste selbst realisiert und alle Rechner beziehen ihre IP-Adresse vom FH-DHCP.

Bei einer Neugestaltung des CAX-Labors (studentischer Schulungsraum) mit einer Neuorganisation des Praktikums- und Übungsbetriebs wurden 2002 Einzelkonten und -Dateibereiche für alle dort arbeitenden Studierenden eingeführt. Dies waren schon anfangs mehrere hundert Konten. Wegen der NT4-Einschränkungen bei „vielen“ Konten (siehe Erläuterung unten) wurde die Handhabung des CAX-Labors in eine eigene Linux-Domain ausgelagert. Die etwas mehr als 30 Labor-PCs blieben aus vielen Gründen — darunter auch der einer FH-Informatikausbildung gut anstehenden Industrie- und Standardnähe — Windows-Workstations mit dem (damals) aktuellen WS-Betriebssystem W2K.

Diese „CAX-Domain“ hatte (außer einem SQID) keine Verbindung zum FH-Netz, siehe Bild 2, oben, und sie erbrachte alle genannten Infrastrukturdienste (DHCP, DNS, SMB) mit Linux-Mitteln selbst.

Sowohl diese im Jahr 2002 vorgenommene Trennung vom FH-Netz und (damit) auch von der Domäne FB3-MEVA als auch die Zweigleisigkeit durch Linux-Server in einer Welt von Windows-Domänen und Workstations erwiesen sich bald darauf als eine äußerst fragwürdige Strukturentscheidung.

Die „Mehrgleisigkeit“ und die bekannten durch das Alter aus den 1960er-Jahren stammenden Grundansatzes erklärten Linux-/Unix-Unzulänglichkeiten führten zu

- einem immensen Verwaltungsaufwand,
- Unzulänglichkeit der an der BO sichtbaren Lösungen und
- Unflexibilität.

Während in nur einer NT4-Domäne (allerdings nur mit Studierendengruppenkonten) die Administrierung des CAX-Labors von einem Dozenten und Assistenten praktisch „nebenher“ mit gemacht werden konnte, erforderte die getrennte Linux-Domain zusätzlich die Dauerbeschäftigung einer fähigen Hilfskraft. Für die erwähnten Dozenten und Assistenten bedeutete dies aber keine Erleichterung im Sinne von „outsourcing", da der zusätzliche Führungs- und Organisationsaufwand sowie die Mehrarbeit in der Praktikumsbetreuung durch Linux-Unzulänglichkeiten den vorherigen „schulungsbedingten“ zusätzlichen Aufwand bei der NT4-Domain-Administrierung weit überstieg.

Alles in Allem führte die genannte unglückliche Strukturentscheidung zu einem Ressourcenverbrauch an unproduktiver Stelle, den das *MEVA*-Lab und das Institut für it-Automation dauerhaft nicht leisten wollen und können.

Erläuterung zu „viele Konten“:
„Viel“ heißt für einen NT4-DC hier leider schon mehr als nur 40 bis 50 accounts. Dabei ist die Zahl der gleichzeitig angemeldeten Nutzer völlig unwichtig. Die bloße Existenz von „vielen“ Konten verlangsamt eine NT-Domäne oft unzumutbar. Der Effekt ist durch eine unglückliche Datenstruktur der ACLs bedingt. Eine W2K3-Domäne kann hingegen ohne Weiteres Tausende von Konten tragen. Damit entfällt das wesentliche Motiv für viele kleine anstatt weniger großer Domänen.

1.4 Domain-Umbauziele

Zu den geschilderten Nachteilen der „Zweigleisigkeit“ kommt für die Domäne FB3-MEVA hinzu, dass NT4 (obgleich im Ansatz mit Unicode, ACLs und vielem anderen immer noch wesentlich moderner als Linux) nicht mehr ganz zeitgemäß ist und in seinen Einschränkungen immer drückender wurde.

Nun boten allerdings W2K- und XP-Server wenig Motive zum einem „Abwandern“ von NT. Dies sehen auch viele andere Profis so: Man findet zum Zeitpunkt des Schreibens (August 2005) in vielen Firmen, einschließlich Banken und Versicherungen, noch ganze „Farmen“ von NT4-Servern. Auch deswegen unterstützt Microsoft — entgegen den seit Jahren ausgestoßenen Drohungen — NT4-Server immer noch; sogar ein W2K3-Domaincontroller kann NT4-BDCs noch „mitnehmen“.

Zu den vielen Gründen zum Bleiben bei NT4 gehörte auch der Hardwareressourcenverbrauch von W2K und (der Spielekonsole) XP. Viele Verantwortliche sind es ja richtig leid, bei jeder neuen Micro-

soft-Betriebssystemvariante jeweils dreifach größere Rechner kaufen zu müssen — und hier lag auch ein großes und gerne genutztes Linux-Reklame-Potential.

Mit Server2003 gibt es nun aber gegenüber NT4-Server zum erstenmal einen echten Fortschritt. Neben vielen zusätzlichen Features und Verbesserungen ist (verglichen mit W2K und XP) auch der Hardware-Ressourcenverbrauch wieder auf ein vernünftiges Maß reduziert worden. Man kann sogar mit Rechnern, auf denen eine W2K-Installation von vornherein abbricht und auf denen manche Linux-Distribution nur unzumutbar läuft, mit Server2003 wieder vernünftig arbeiten. Die Erfahrungen im *MEVA*-Lab zeigen, dass ein Rechner, wie alt und klein auch immer, der ein NT4 halbwegs laufen lässt dies auch (und oft besser) mit Server2003 tut. Insofern kann man W2K3 (Server2003) mit gutem Erfolg auch als WS-Betriebssystem einsetzten (siehe weiter unten bei Labor). Wenn Microsoft den Server2003 mit den nächsten Versionen und Servicepacks auch in dieser Hinsicht nicht wesentlich verschlechtert, dürften die Tage von NT4 nun doch bald gezählt sein.

Damit standen im *MEVA*-Lab folgende Ziele an:

Ziel A) Umstellung der NT4-Domäne FB3-MEVA auf Server2003-DCs

und

Ziel B) Umstellung der CAX-Labor-Domäne von Linux auf Server2003-DCs.

Für das Ziel B) kommen grundsätzlich zwei Ansätze in Frage

- eine gesonderter aber FB3-MEVA vertrauende (Labor-) Domäne

oder

- alles mit einer Domäne, sprich mit der Domäne FB3-MEVA allein.

Für das Ziel A), also die Umstellung der Domäne FB3-MEVA, galten folgende harte Bedingungen:

- Workstations und Server bleiben im FH-LAN.
- Workstations und Server müssen die unbeeinflussbaren FH-Infrastrukturdienste DHCP, WINS und DNS nutzen.
  Insbesondere letzteres stellt ein ernsthaftes Problem im Zusammenhang mit AD dar.
- Erhalten aller Nutzer- und Computer-accounts.
  Dies musste 100%ig gelingen, da an diesen fachbereichsweit (und teilweise darüber hinaus) zahlreiche Zugriffsrechte (in ACLs) hängen.
- Erhalten aller Nutzerdateien, auch derjenigen auf den Domain-Controllern.

Für das Ziel B), also den Umbau des CAX-Laborbereichs, galten folgende Forderungen, die allerdings jeweils nicht ganz so zwingend sind:

- Die CAX-Labor-Workstations sollten flexibel von der Domäne aus verwaltet werden.
- DNS und evtl. auch DHCP und dergleichen sollte für die Workstations möglichst durch die Domäne bereitgestellt werden.
- Der Internet-Zugang für die Workstations muss an zentraler Stelle organisiert werden.
  Die bisherige SQID-Lösung ist prinzipiell ausreichend. Es besteht aber die Forderung (auf für jeden Dozenten einfache Weise) den Workstations des Schulungsraums zeitweise den Internetzugang abzuschalten.
  Dies scheint für den Internetzugang freigegebenen Rechnern direkt am FH-Netz zu widersprechen *).
- Authentifizierung der studentischen Nutzer mit ihrem zentralen FH- (mail-) account via FH-DVZ-LDAP bzw. SSO.
- Übernahme der Dateien der (Linux-) Nutzer von Linux-Servern nur auf Anforderung.

Der erste Schritt musste also A) sein, das heißt die Migration der Domäne FB3-MEVA nach Server2003-DCs unter den genannten „harten“ Bedingungen; siehe folgendes Kapitel 2. Hierbei brauchte das CAX-Labor, also das Ziel B) Kapitel 3 ab Seite 15, zunächst nicht berücksichtigt werden.

Erläuterung *): „Für den Internetzugang freigegeben“ heißt, dass der betreffende Rechner beim Firmen- (sprich FH-) Proxy als „darf mit http und Konsorten nach draußen gucken“ eingetragen ist. Ohne diese (hier an letztlich der Rechner-MAC-Adresse hängenden) Freigabe kann ein Rechner niemals „rausgucken“.

Und mit dieser Freigabe lässt sich diese Möglichkeit auf diesem Wegen nicht mehr einfach unterbinden, zumindest nicht im Sinne eines kurzfristigen, vorübergehenden Ausschaltens.

2 Migration der Domäne FB3-MEVA

Wie bereits erwähnt, lag eine der zu erwartenden Hauptschwierigkeiten im unbeeinflussbaren DNS der FH Bochum. Dieses (Linux-basierte) DNS unterstützt AD nicht, akzeptiert keine dynamische Serviceeinträge von DCs und dergleichen; es muss aber gleichwohl für eine AD-Domäne in diesem Netz genutzt werden.

Einige Fachleute und auch Äußerungen von Microsoft bezeichnen das Einrichten einer AD-Domain unter diesen Bedingungen als schwierig bis unmöglich. Zitat Microsoft-Support, 2004:

„no influence on company DNS?" ⇒ „forget it!"

Dennoch war die eigentliche FB3-MEVA-Migration mit einer guten Woche Arbeit zu zweit Mitte August 2005 im Wesentlichen und unter Einhaltung der genannten „harten" Bedingungen erfolgreich abgeschlossen.

Dies war aber nur durch monatelange intensive Vorbereitung bis hin zu einigen „Trockenexperimenten" mit zwei Servern und zwei Workstations möglich, sowie dank der Unterstützung durch Kenner der Materie in der DVZ und im Fachbereich Informatik.

2.1 Installation / Upgrade

2.1.1 Vorbereitung

Die Schritte zur Vorbereitung wurden „lehrbuchmäßig" durchgeführt:

- Probe-W2K3-Installation auf den Ziel-Servern außer auf dem NT4-PDC (PD321S).
- Zwei NT4-BDCs auf der neuen Server-Zielhardware (SNI Primergy, PD322S, PD323S).
- Plattenabbild des NT4-PDC (PD321S) erstellen und einlagern.
- „Trockenübung" des Vorgangs mit „Spieldomänen".

Die immer empfohlene Probe-W2K3-Installation soll den Effekt verhindern, dass alles Andere vorbereitet ist und sich dann rausstellt, dass man W2K3 auf dem Zielrechner nicht installieren kann. Dieser Schritt scheint unnötig. Wie schon erwähnt, läuft W2K3 ja auf vielen Rechnern, auf denen „sonst fast nix geht" — bis hin zu Linux. Bei Rechnern mit hardwaremäßigen Besonderheiten, HP, RAID, besondere Netzwerkkarten, FO, etc., sollte man aber nie darauf verzichten. Diese „Übung" kostet dank der komfortablen und schnellen W2K3-Server-Installation auch vergleichsweise wenig Zeit, und sie erwies sich im Zusammenhang mit den RAID-Controllern der eingesetzten SNI-Server als wirklich nötig.

Die mittleren beiden der oben genannten Schritte sollten die harte Nebenbedingung „Keine Nutzer- und Computerkonten verlieren" sicherstellen. Ursprünglich sollte nicht vor einem mindestens dreimonatigem erfolgreichem Betrieb der auf W2K3 umgestellten Domäne der letzte Weg zurück zum alten (ja schließlich jahrelang betriebsbewährten) NT4-Zustand abgeschnitten werden.

Das Erstellen von zusätzlichen BDCs, die man auch einmotten und bedarfsweise zum PDC befördern kann, ist sinnvoll und bis auf die Umstände einer NT4-Server-Installation einfach. (Hier braucht man ja noch Disketten und mindestens fünfmal so lang wie für eine W2K3-Installation.)

Das Motiv, ein Plattenabbild des bisherigen PDC zu erstellen, lag darin, dass die Beförderung vom BDC zum PDC bei NT4

a) eine Einbahnstraße ist,

b) es nicht mehrere PDCs in einer NT4-Domäne geben kann und dass

c) die Hochrüstung einer Domain auf W2K3 am PDC erfolgen muss.

Bei W2K3 gibt es die Unterscheidung PDC / BDC in dem strengen NT-Sinne nicht mehr.

Es ergab sich aber, dass beim Erstellen der Plattenabbilder des NT4-PDCs (Server PD321S) mehr Schaden und Risiko als Nutzen entstand, da die betreffenden Werkzeuge mit dem relativ alten no name-PC und seinen I/O-Bussen nur bedingt klar kamen. Am Ende konnte man froh sein, den alten NT4-PDC wieder funktionstüchtig zu haben.

Von diesem Punkt der Vorbereitungen ist also abzuraten. Nach den gemachten Erfahrungen erscheint es besser so vorzugehen:

Auf dem neuen „Haupt-DC“ NT4-Server installieren und ihn zum BDC machen (wenn er es nicht schon eh‘ ist). Dann sofort den alten PDC offline nehmen und den „Ziel-Server“ zum NT4-PDC befördern und dann nach W2K3 hochrüsten. Siehe hierzu die Anmerkungen zu „single master Rollen“ weiter unten.

Die „Trockenübung mit einer Spieldomäne“ hat sich hingegen als entscheidend erwiesen, da man so alle möglichen DNS- und DHCP-Probleme mit der Firmen- (sprich hier FH-) Infrastruktur durchspielen kann ohne einen Server mit wichtigen Kontendaten anzufassen oder indirekt die ganze produktive Domäne durch Aufdatvorgänge aus einem evtl. verdorbenen DC heraus zu gefährden.

2.1.2 Durchführung .

Die Durchführung der Migration (Details zu einzelnen Punkten siehe z.T. weiter unten) geschah mit diesen Schritten:

- alle BDCs (PD322S, PD232S) offline (durch Ziehen des LAN-Kabels),
- Upgrade des PDC (PD321S) von NT4 auf W2K3,
- Einrichten von Netzwerk, DNS, und remote terminal server, Java, Framework, MEVA-Standard-Umgebungsvariablen etc. auf dem PD321S,
- Test, ob Clientrechner noch an der (nun W2K3-) Domäne FB3-MEVA funktionieren,
- Einrichten eines zweiten DC auf einem neuen Server (PD324S, SNI Primergy, RAID)
- Nacharbeiten (remote terminal, Java, Framework, Umgebung, etc. genau wie beim PD321S)
- Einrichten eines dritten DC durch W2K3-Neuinstallation auf einem bisherigen BDC (PD323S)
- Übertragen aller Nutzerdaten von PD321S (alter PDC) und von PD322S (alter und noch NT4-BDC) auf PD324S und PD323S (mit Robocopy.exe wegen der ACLS)
- Änderung der Anmeldungs-Skripte, so dass Nutzer sich bevorzugt mit PD324S und ersatzweise PD3232S, statt bisher PD321S und ersatzweise PD322S, verbinden
- PD322S offline (NT4-BDC, letzte Rückfallrettung)
- PD321S offline (W2K3-DC, Rückfallrettung, falls weitere Arbeiten die nun W2K3-Domäne FB3-MEVA unbrauchbar machen)
- Beseitigung der PD21S-Bezüge (DNS) bei den anderen DCs

Anmerkung zum (vorletzten) Punkt „PD321S offline“:
Der ehemalige NT4-PDC PD321S wurde als erstes hochgerüstet. Dieser hardwaremäßig veraltete Rechner sollte ja baldmöglichst außer Betrieb genommen werden. Wenn auch W2K3 die harte Unterscheidung PDC / BDC nicht kennt so gibt es in einer W2K3-Domäne doch einige single master Rollen sowie Rollen, die üblicherweise nur einer der DC zugewiesen bekommt. Durch die ungünstig gewählte Hochrüststrategie waren zunächst alle diese Rollen beim letztlich „abzuklemmenden“ PD321S. Dies hatte negativen Konsequenzen sowie Rollenübertragungen und -zuweisungen zur Folge; siehe folgendes Kapitel 2.1.3.
Letztere waren nicht ganz unkritisch, da man ja kurz nach dem ersten ernsten Umstieg von NT nach W2K3 ja zunächst unvermeidlich AD-Anfänger ist. Hier galt mal wieder: Man lernt nur durch Leiden.

Anmerkung zu offline / online Setzen an sich:
Diesen Vorgang kann man bei allen Windows-Servern und -WSs durch Ziehen und Stecken des Netzwerkkabels (+ Nichts) zuverlässig darstellen. Bei Linux-Systemen führt so was hingegen gerne in einen Absturzzustand ohne Erholungsmöglichkeit (außer durch re-boot).

2.1.3 Ehemaligen PDC off line setzen — single master Rollen .

Der erste hochgerüstete ehemalige NT4-PDC, PD321S, bekommt durch diesen Vorgang in der nun W2K3-Domäne einige Rollen allein. Die geplante Außerbetriebsetzung dieses veralteten no name Rechners wurde durch einfaches off-line-Nehmen (mehrfach) geprobt. Was man vorher (und besser in einem Zug als in „Lern-„ Schritten) tun muss, ist im folgenden aufgeführt.

Das (erste) off line Nehmen ist erst ohne Schaden, sprich Funktionseinschränkungen, möglich, nachdem der GC auf die anderen DCs repliziert wurde. Standardmäßig entsteht der GC nur auf dem

ersten eingerichteten W2K3-DC. Im (vorliegenden) Fall einer kleinen Domäne mit einem bis drei DCs ist es sinnvoll, GC auf allen DCs laufen zu lassen.

Letztlich ergaben sich folgende Rollenübertragungs- bzw. Verteilungsschritte auf die weitern DC — hier zunächst auf PD324S und PD323S:

- GC auf alle DCs replizieren.
- Primary DNS-Server in allen DCs von PD321S auf PD324S umstellen.
- Zeitdienst (W32Time) auf NTP mit dem FH-NTP-Server als zentralen DCF-Master auf allen DCs einrichten. Derer Zeitquelle (in ihrer Rolle als Client) ist der FH-Zeitserver NTP1.
- Alle single master Rollen, insbesondere die des PDC-Emulators, von PD321S auf PD324S übertragen.

Tabelle 3 gibt einem Überblick über die DCs und ihre Rollenwechsel bei der Hochrüstung der Domäne FB3-MEVA.

Name	alte Funktion	Übergang	neue Funktion	Endzustand
PD324S	nicht vorhanden	neu installiert, Rollen übertragen	W2K3- (P) DC	erster DC
PD323S	NT4-BDC	neu installiert	W2K3-DC	zweiter DC
PD322S	NT4-BDC	keine Änderung neu installiert *)	NT4-BDC W2K3-DC *)	offline DC, file
PD321S	NT4-PDC	upgrade von NT4 auf W2K3	W2K3-DC	außer Betr.

Tabelle 3: FB3-MEVA-DCs und ihre Rollen bzw. Rollenwechsel

Anmerkung *): Nach anderthalb Wochen erwies sich der Betrieb des bisherigen FB3-MEVA-Domänen-Funktionsumfangs unter W2K3 als so stabil und zufriedenstellend, dass der Rückweg nach NT4 abgebrochen wurde. PD322S bekam durch Neuinstallation eine ähnliche Funktion wie PD323S und die des primären file servers für die Studierendenkonten.

2.2 Besonderheiten

2.2.1 Piling on

Hintergrund:
Man kann einen W2K3-DC so konfigurieren, dass er sich Clientrechnern gegenüber als NT-DC ausgibt und so Clients ausschließlich das (ab NT4_SP4 ja recht gute) NT-challenge-response Authentifizierungsverfahren anbietet. Ein Client-Rechner mit W2K oder höher, dem ein entsprechender DC ein von Microsoft nun bevorzugtes Verfahren (Kerberos) auch nur ein einziges Mal angeboten hat, wird sich nie mehr an einem NT-Server anmelden.
Um es gleich zu sagen: Dieses unkonfigurierbare „Einbahnstraßen“- (oder Drogensucht-) Verhalten der Client-WS ist eine Microsoft-typische Kundengängelung (gelinde gesagt).

Der Effekt heißt “piling on”, weil sich aufgrund des geschilderten W2K-Clientverhaltens nach Hochrüsten auch nur eines von n Servern, solche Clients nie mehr bei den n-1 Servern anmelden, sondern nur noch den so nun selbst oder in seiner Netzwerkanbindung möglicherweise überlasteten Einen belagern.

Verfahren:
Solange man aus Lastverteilungsgründen in der Hochrüstungsphase dieses “piling on” vermeiden muss, oder solange man befürchtet, nach einer Katastrophe evtl. zur alten NT-Domäne rückkehren zu müssen, muss man folgendes noch vor (!) der Hochrüstung des NT-Servers nach W2K3 in der Registry einstellen:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters\

Wert: NT4Emulator DWord = 1

Dies sorgt dafür, dass sich der (künfige) W2K3-Server wie NT gebärdet. Löschen oder auf 0 setzen schaltet das W2K3-Verhalten ein. Der erste Grund (Anmelde-Lastverteilung) spielt in der FB3-MEVA-Struktur praktisch keine Rolle; die “reuemütige” Rückkehr zu einer NT-Domäne sollte aber als letzte

Rückfallstrategie zunächst offengehalten werden (siehe aber Anmerkung am Ende des letzten Kapitels).

Problem 1:
Bei einem so konfigurierten W2K3-DC können zwar Workstations der Domaine beitreten. Es ist aber unmöglich, dass weitere DCs hinzugefügt werden. Dieser undokumentierte Effekt wurde erst nach sehr langwierigem Suchen nach anderen möglichen Ursachen entdeckt. Während des Beitritts eines neuen DC (und dort AD einrichten) muss "NT4Emulator" auf den vorhandenen DCs abgeschaltet werden. Falls man auf die Verhinderung von "piling on" noch nicht verzichten kann, muss man also dafür sorgen, dass sich die betroffenen Workstations in diesem Zeitraum auf keinen Fall anmelden — ein weiterer Fall für Nachtarbeit.

Hinweis / Klarstellung:
Da NT4Emulator-Schalterstellung hat nichts mit der Frage zu tun, ob sich beispielweise NT4-Workstations anmelden können. Die Server bieten mehrere Authentifizierungsverfahren an. „piling on" hat nur mit dem Client- „Drogensucht-" Verhalten zu tun. Mit dieser Willkürmaßnahme möchte Microsoft offenbar alle Server mit NT4-Verhalten durch einmal süchtig gemachte Clients unverwendbar machen und so ausrotten.

Einige Tage nach der Domänenumstellung wurde beschlossen, den „piling on"-Schalter umzulegen und so die überwiegenden Zahl von PCs und Laptops mit Betriebssystem < W2K auf das modernere Anmelde-Verfahren (endgültig) umzustellen. Die Gründe waren:

- Anmeldemöglichkeit für „Alt-Clients" ist davon unabhängig gegeben (wurde getestet und siehe obigen Hinweis)
- Fehlervermeidung beim Warten von DCs
- Vorteile des moderneren Authentifizierungsverfahrens
- Nach nur guten Erfahrungen bestand keine Absicht mehr (egal nach welchen Ereignissen) den alten NT4-Zustand wieder herstellen zu wollen

Das Umlegen des „piling on"-Schalters brachte keine sichtbare Wirkung für die Anwender der Clients, also auch keine Nachteile. So ergaben sich angesichts der ganzen — irgendwie nicht leicht durchschaubaren — Affaire die Fragen

- Warum nicht gleich? Und:
- Hat sich überhaupt was geändert?

Problem 2 :
Eine unerfreuliche Nebenwirkung zeigte allerdings, dass die Antwort auf die letzte Frage „Ja" ist. Ein Labtop, der Mitglied der Domäne FB3-MEVA ist, konnte und sollte sich außer Haus immer in einer Arbeitsgruppe eines kleinen Firmennetzes bewegen. Dies ging seit der piling-on-Abschaltung (und nach nur einer Anmeldung im FH-Netz) auf einmal nicht mehr. Statt der braven Arbeit im erwähnten Firmennetz, gab nur noch Fehlermeldungen des Sinnes „Wo ist mein Anmeldeserver?" — sprich „Wo ist meine Droge (Kerberos)?"

Die oben geschilderte Marketing-Willkür von Microsoft macht also Reisearbeitsmöglichkeiten von Labtops kaputt — und im konkreten Fall war und ist das noch immer ... großer Mist. Dies sollte man bei der NT4-Emulator-Entscheidung mit bedenken.

2.2.2 DHCP .

Wegen der Bedingungen der Firmen- (FH-) Infrastruktur muss die IP-Adresse der DC und WSs nach wie vor vom FH-DHCP bezogen werden (DNS nicht; siehe Kap. 2.2.3). Bei der Einrichtung von AD bzw. des Rechners als DC wird hierzu zwar zweimal gemeckert, aber es geht dann doch.

Man muss (und kann) sich an dieser Stelle fest darauf verlassen, dass das FH-DHCP diesem Server niemals eine andere IP-Adresse (die dann auch das FH-DNS liefern würde) gibt. Wäre diese Bedingung nicht gegeben, so nützte das feste Eintragen der aktuell vergebenen IP-Adresse ja auch nichts.

Als „alternative" IP-Konfiguration kann aber das eingetragen werden, was das FH-DHCP liefert. Dann geht manches auch noch bei kurzzeitigem Ausfall des zentralen DHCP oder der Verbindung dorthin.

2.2.3 DNS .

Active Directory-Domänen ohne vollen Einfluss auf das DNS stellen, wie schon mehrfach erwähnt, eine Grundschwierigkeit dar. Hier ist gezeigt, wie es ging und geht.

Rechnername	IP-Adresse	Weiterl.	Haupt-Funktion	Betriebssystem
PD324S	195. 37.168.187	pav032	FB3-MEVA-DC	W2K2 SrvEnt
PD323S	195. 37.168.164	pav032	FB3-MEVA-DC	W2K2 SrvEnt
PD322S	193.175.113.245	pav032	file server, DC	W2K2 SrvEnt
pav032.fh-bochum.de	193.175.112.8	- (?)	FH-Bo DNS	Solaris

Tabelle 4: DNS-Server

Alle DCs sind (notwendigerweise) DNS-Server, Anfragen, die sich außerhalb der Domäne liegendes beziehen, leiten sie an einen der FH- (Firmen-) DNS-Server (pav032.fh-bochum.de) weiter; siehe Tabelle 4.

Alle Rechner sind (notwendigerweise) DNS-Clients; dies gilt auch für DCs. Die Client-Einstellungen sind:

DNS-Client (TCP-IP-Eigenschaften) auf einem DCs:

- DNS nicht via FH-DHCP beziehen
- Erster DNS-Server: DC selbst
- Zweiter DNS-Server: anderer DC
- Dritter DNS-Server: pav032.fh-bochum.de (Eintrag könnte wg. Weiterleitung entf.)

DNS-Client (TCP-IP-Eigenschaften) auf den Clients (WS) und weiteren DCs:

- DNS nicht via FH-DHCP beziehen
- Erster DNS-Server: Ein DC (PD322S .. PD324S)
- Zweiter DNS-Server: Ein jeweils anderer DC (PD324S .. PD322S)
- Dritter DNS-Server: für (Büro-) Rechner, die auch bei Ausfall der Domäne arbeiten sollen / können evtl. pav032.fh-bochum.de
  (Eintrag kann wg. Weiterleitung an sich entfallen.)

Die DNS-Client-Eigenschaften auf den WS der Domäne können nach und nach geändert werden. Mit den vom FH-DHCP gelieferten Einstellungen funktioniert das Meiste auch, nicht allerdings einige (AD-) Verwaltungsarbeiten an dem betreffenden Computerkonto selbst.

Bei den Servern gilt: Nach Einrichten des AD ist der oben geschilderte „DNS-Selbstbezug“ notwendig. Bei Neuinstallation eines Servers gilt: Vor dem Einrichten von AD im Rahmen der Einrichtung als „weiterer domain controller“ muss einfach ein anderer DC als DNS-Server gesetzt werden.

2.3 Nacharbeiten an der Domain FB3-MEVA .

2.3.1 Windows-Update .

Die DCs wurden auf den FH- (Firmen-) Updateserver mit WSUS anstelle des IE-Zugriffs direkt nach MS umgestellt. WSUS wird von der FH-DVZ dankenswerterweise zentral zur Verfügung gestellt.

Um die WSUS-Verwendung einzustellen, muss man an dem betreffenden Rechner mit Administrator-rechten angemeldet sein. Mit dem Gruppenrichtlinien-Editor gpedit.msc navigiert man zu
Richtlinien → Administrative Vorlagen →...→ Windows-Update.

Dort konfiguriert man

Interner Pfad = http://firmenWsusServer (z.B. http://PC0022, zweimal)

Updates = 3 (download und Nachricht)

Neustart = nicht automatisch (i.A. empfehlenswert)

Die Einstellungen gelten und funktionieren für Server (DC) und WS gleichermaßen. Die Erfahrungen sind gut, und mit „Einstellung 3“ behält man ja weiterhin alle Kontrolle über den Vorgang. Allerdings muss man sich mit diesen Einstellungen die Rechner auch immer mal anschauen (remote genügt).

Mit WSUS wurde nicht nur das („Riesen“-) W2K3-ServicePack 1 auf alle Server (DC) und viele WS geladen sondern auch zahlreiche nachfolgende MS-Sicherheits-Updates. Probleme gab es bis dato (Oktober 2005) nicht.

Servicepack 1 macht allerdings auf Rechnern, auf denen der Terminaldienst installiert ist „Sperenzchen“. Hier drohen „ewig“ laufende und lizenzmäßig korrekte Installationen auf einmal mit Einstellung der Arbeit „nach 121“ (sic! gemeint sind wohl Tage). Oft aber nicht immer half es, den ja vorhandenen und bisher gefundenen und genutzten Terminaldienst-Lizenzserver auf den Clients noch mal explizit einzutragen. Diese (gewollte?) Belästigung durch das SP1 hat aber nichts mit WSUS zu tun.

Nach hinreichender Erprobung der jeweiligen Updates und Servicepacks möchte man i.A. nicht mehr zum Vorzustand zurückkehren. Sodann kann man dann die „Rückfallverzeichnisse“ `C:\WINDOWS\$***$` löschen.

2.3.2 Skripte

Die Anmelde-Skripte, insbesondere homeAnm.bat, Listing 11 ab Seite 24, für die wenigen “Kernteam-” Benutzer, wurde auf PD324S vor allem dahingehend geändert, dass die üblichen Netzlaufwerke Z: und P: nun mit PD324S und ersatzweise mit PD323S verbunden werden. Der übliche Ort solcher Skripte ist nun (unter W2K3)

```
C:\WINDOWS\SYSVOL\sysvol\FB3-MEVA.fh-bochum.de\scripts
```

Die Skript-Replikation und Verwendung in den Clients funktioniert absolut problemlos — ganz im Gegensatz zu NT, ein echter Fortschritt also.

Zum Anmeldeskript für studentische Nutzer siehe weiteres unten in Kapitel 3.

2.3.3 Pfade und Tools

In der Systemsteuerung wurde (für Alle) der Suchpfad für Programme (vorne!) ergänzt:

```
C:\bat;c:\programme\util;C:\programme\jdk\bin;C:\WINNT\sys.....
```

Dies ist der bewährte FB3-MEVA- bzw. MEVA-Lab-Standard.

Der (hintere) Rest blieb. Insbesondere zeigte es sich, dass man das suspekte WBem nicht mehr „abknapsen“ darf, da ansonsten einige Installationen und (WSUS-) Updates nicht mehr funktionieren.

In `c:\programme\util` wurden Programme RoboCopy, EditPad, Shutdown, SetACL und ähnliches getan. Dies gilt mit sinngemäßen Ausprägungen für alle DCs und WSs.

2.3.4 Java

Auf allen Servern wurde Java 5 in der Version JDK 1.5.0_04 installiert und mit dem Framework de.a_weinert... und allen Dokumentationen ergänzt. Benutzte Installationsdateien:

```
17.08.2005  11:46   59.465.592  jdk-1_5_0_04-windows-i586-p.exe
11.11.2004  09:00   45.635.523  jdk-1_5_0-doc.zip  // JDK-Doku
24.10.2005  09:35    9.527.239  erg.zip      // framework etc.
```

Dies gilt für alle DC. Auf WSs, insbesonderen denen der Labore und Schulungsräume, wurde als Standard-Java (d.h. in C:\programme\jdk\) 1.4.2_09 installiert. Dies geschieht, um Java-Anfänger nicht gleich mit Java 5 zu konfrontieren und um einige Java-basierende kommerzielle Tools „mitzunehmen“; die sind nicht alle Java 5-geeignet. Die hierfür benutzten Installationsdateien sind:

```
17.08.2005  11:41   55.611.765  j2sdk-1_4_2_09-windows-i586-p.exe
01.09.2003  16:04   34.397.778  j2sdk-1_4_2-doc.zip  // JDK-Doku
24.10.2005  09:35    9.527.239  erg.zip  // framework etc. (selbe Datei)
```

(oder jeweils neuere Versionen)

Mit beiden Java-Versionen funktionieren alle Java-basierten Dienste (Utilities) auf allen DCs und WSs.

2.3.5 Sophos .

Auf allen DCn und WSs wurde in C:\bat das Skript klinkVir.bat, Listing 9 auf Seite 22, ergänzt.

Durch Aufruf (klinkVir) dieses Skripts von Hand mit Administratorrechten wurde der Sophos-Antivirendienst erstmalig installiert, falls er auf dem jeweiligen Rechner noch nicht vorhanden war.

Desgleichen wurde dieses selbe Skript (klinkVir.bat) als täglich dreimal laufende Task auf allen DCn und WSs eingerichtet. Es holt (mit Update.java) die jeweils neuste Version von dem FB3-MEVA-Server PD310S. Dieser wiederum bedient sich (mit fast dem gleichen Skript) beim Firmen- (FH-) Sophos-Server. Bei Änderung der Sophos-Lizensierungsverhältnisse muss das Verfahren u.U. geändert werden, wenn auch evtl. nur auf dem PD310S.)

Diese automatische Task muss mit Administratorrechten eingerichtet werden. Für die monatlich fälligen Neuinstallation sowie für das Stoppen und Starten des Dienstes nach einer täglichen Nachlieferung von Identifikationsdateien genügen normale Nutzerrechte nicht.

2.3.6 Backup .

Im Backupserver (PD382S) wurden die Properties für die Java-Applikation FileServices (Aufdat-Server) so verstellt, dass nun PD324S und PD323S (statt bisher PD321S und PD322S) gesichert werden. Siehe Listing 10 ab Seite 23.

2.3.7 Weitere Einstellungen .

Bei Server 2003 sind [angeblich] lokale Administratoren, die an „ihrem“ der Domäne zugehörendem Rechner angemeldet sind, (anders als bei NT4) grundsätzlich auch Domain- und Enterprise-Administratoren. Dies ist in einem Betrieb, in dem Studierende bei Projekten gelegentlich Administratorrechte auf Experimentalrechnern brauchen, unerwünscht. Bei der vorliegenden Migration von NT4 schien dies allerdings nicht der Fall zu sein.

Dieser Punkt bedarf noch einer genauen Klärung bzw. Beobachtung.

Um bei nun mehr Konten für Nutzer und Computer die Übersicht zu behalten, wurden Organisationseinheiten (OUs) für Rechner in Schulungsräumen und für Studierende angelegt:

- caxLabWS für Computer (WS) des Schulungsraums,
- mevaStGrp für Gruppen-Anmeldekonten und deren administrative Konten,
- fb3Stud für Studierenden-Einzelkonten und deren Rechte-Gruppen,
- SchrottKonten für nicht mehr benötigte Konten (gelegentlich „recyclen” oder vernichten)

Siehe weiter unten hierzu auch das Bild 8 auf Seite 17.

2.4 Résumée .

Alles in Allem war die Umstellung der Domäne FB3-MEVA von NT4 auf W2K3 ein voller Erfolg, nur ein paar Kleinigkeiten waren vier Wochen danach noch zu klären bzw. nachzuarbeiten. Die Clients und Anwender hatten weitestgehend entweder nur Vorteile oder sie haben von der ganzen Sache nichts bemerkt — und das ist ja auch schon was.

Als Ärgernis blieben letztlich nur die notorischen Microsoft-Willkürmaßnahmen à la Client-Anmeldeverhalten sowie immer noch vorhandene Lücken in der Werkzeugausstattung, selbst nachdem man alle möglichen „ressource-net-admin-tool-bastel-kits“ durchgeklaubt hat. Warum ist bei „Server“ nicht Alles dabei, was man als Administrator so zum Administrieren und zum Automatisieren (!) von Administrieren benötigt.

Festzuhalten bleibt aber, dass W2K3 (auch) beim letzten Punkt drei Klassen besser ist, als alles davor.

3 Labornetz / Schulungsraum / Studierendenkonten

3.1 Strukturelles Konzept

Die Organisation von Studierendenkonten, Labors und Schulungsräumen geschah bisher in einer weitgehend abgeschotteten „CAX-Labor-Domäne“ auf Linux-Basis, vgl. Bild 2 auf Seite 4. Für die Konsolidierung kamen die in Kapitel 1.4 ab Seite 5 geschilderten Ansätze in Frage und es galten u.A. die Anforderungen:

- Die CAX-Labor-Workstations sollten flexibel von der Domäne FB3-MEVA aus verwaltet werden können.
- DNS und evtl. auch DHCP und weiteres soll für die Workstations durch die Domäne bereitgestellt werden.
- Der Internet-Zugang für die Workstations soll an zentraler Stelle organisiert werden. Die bisherige SQID-Lösung ist prinzipiell ausreichend. Allerdings sollte auf für jeden Dozenten einfache Weise der Internetzugang nach außen für die Schulungsrechner abgeschaltet werden können.
- Authentifizierung der studentischen Nutzer mit ihrem FH-mail-account via DVZ-LDAP.
- Übernahme der Dateien der (Linux-) Nutzer von Linux-Servern nur bei konkretem nachgewiesenem Bedarf.

Intensive Planung und leidvolle Experimente, bedingt vor Allem durch „legacy”-„ Software wie EPlan, Matlab, AutoCad sowie WinCC und Konsorten, insbesondere mit deren Lizenzserver und andere Plagen betreffenden Sonderanforderungen, führten schließlich zu folgenden Strukturentscheidungen:

- Alles mit einer Domäne, sprich mit FB3-MEVA allein.
- PD322s wird der DC, der (als LAN-mäßig naheliegender) die Schulungs-Workstations „betreut“.
- PD322s wird (erst mal auch) File-Server für die Studierendenkonten
- Die CAX-Labor-Workstations kommen ins FH-LAN und beziehen ihre Adresse vom FH-DHCP
- Die CAX-Labor-Workstations nutzen die DCs als DNS-Server (PD322S an erster Stelle)
- Die CAX-Labor-Workstations werden (FH-zentral von der DVZ) für den Internetzugriff nach außen freigegeben.

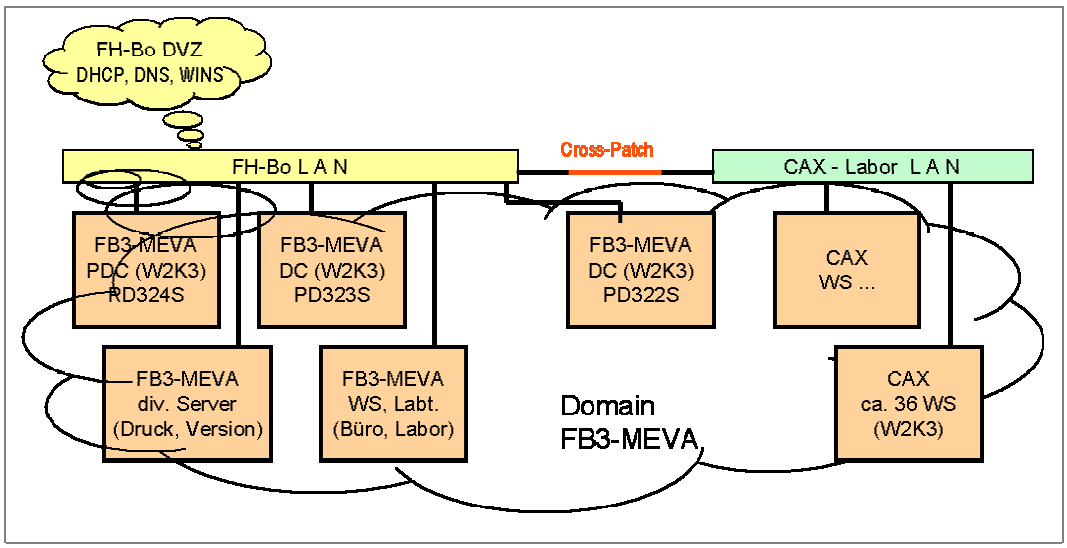

Bild 5: Neue Domänenstruktur FB3-MEVA mit Schulung (CAX)

Bild 5 zeigt die Vereinfachung der neuen Struktur gegenüber der Ausgangslage von Bild 2 auf Seite 4.

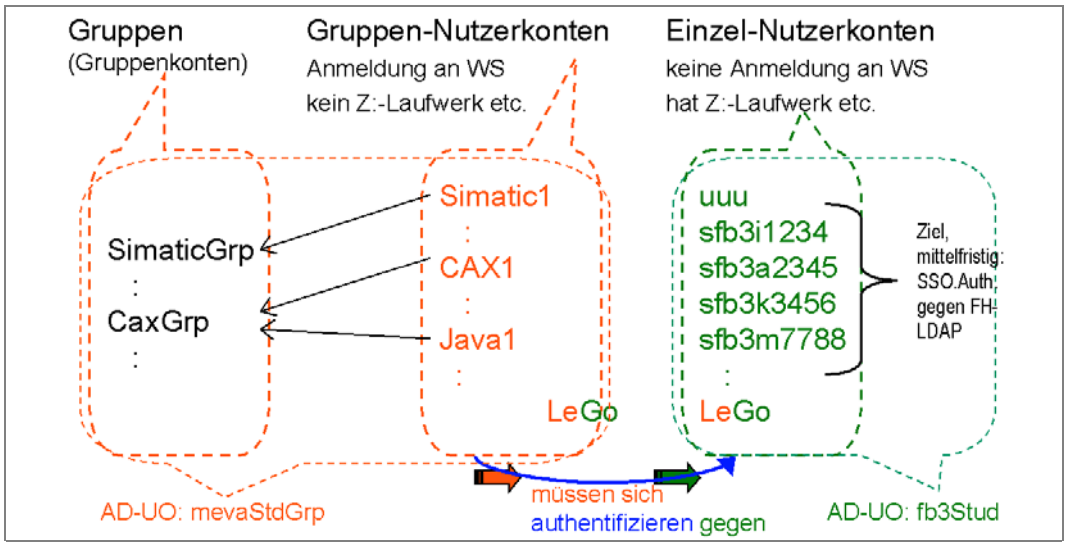

Bild 6: „Gruppenbenutzer“ (wenige) und (sehr viele) studentische Benutzer (Prinzip).

Für die Studierendenkonten und den Praktikums- / Schulungsbetrieb gilt folgendes, siehe auch Bild 6:

- Jeder Studierende bekommt ein individuelles Konto (sfb3xyz) in der Domäne
- Der Kontennamen entspricht dem Namen des FH- email-Kontos, das zentral von der DVZ in einem LDAP-Server verwaltetet wird.
- Das Passwort des domain-Kontos wird mit dem passenden gleichnamigen FH-LDAP-Konto synchronisiert.
  Dies geschieht (mindestens) bei jeder Benutzeranmeldung an einer WS.
- Mit diesen FB3-MEVA-Einzelkonten werden die individuellen file-server-Rechte (acls), quota etc. dargestellt.
- Die Anmeldung an irgendeinem Rechner mit diesen (Studierenden-) Einzelkonten (als WS-Anmeldekonto) wird unterbunden.
- Für die Anmeldung zur Arbeit an den Labor-WS gibt es „Gruppenbenutzer“ (cax1, java1, matlab1 und ähnliche).
  Aus menschlicher Benutzersicht sind dies (Arbeits-) Gruppenkonten.
  Aus Windows- (AD-) Sicht sind diese Konten Benutzerkonten (und keine Gruppenkonten, vgl. Bild 6) mit fest zugewiesenen serverbasierten Profil und Anmeldeskript.
- Bei der Anmeldung mit einem solchen „Gruppennutzer“ wird via Skript studGrup1Anm.bat, Listing 12 ab Seite 26, und einer Java-Anwendung (LogAlert.java, Bild 7) eine zusätzliche individuelle Authentifizierung gegen das Einzelkonto (siehe erster Punkte oben) verlangt.
- Durch die Anwendung werden gegebenenfalls dann auch die Verknüpfung zu den individuellen Ressourcen (file server, „Z:-Laufwerk“, etc.) hergestellt.
- Ferner wird (von LogAlert.java) eine Verbindung mit lediglich Leserechten zu einer „Gruppennutzer“ -Ressourcen (file server, „Y:-Laufwerk“) hergestellt.
- Mit den letzten beiden Punkten werden auch weitere Anmelderechte bzw. -beschränkungen überprüft, siehe auch Bild 8.
- Die Einzelkonten und die Gruppennutzerkonten kommen in getrennte OUs.
  Beide OUs haben keine speziellen Gruppenrichtlinien.

Auf die Verwendung von W2K3-Gruppenrichtlinien, und damit auch auf deren durchaus vorhandenen Komplikationen und Nebenwirkungen, konnte (und sei es vielleicht nur zunächst) verzichtet werden, da man es trotz Hunderten von studentischen Benutzern in dieser Struktur mit weniger als einer Handvoll „Arbeitskonten“ und festen Profilen zu tun hat. Mit diesen Profilen sowie den Anmeldeskripts und -tools kann man (wie im Folgenden gezeigt) alles robust regeln.

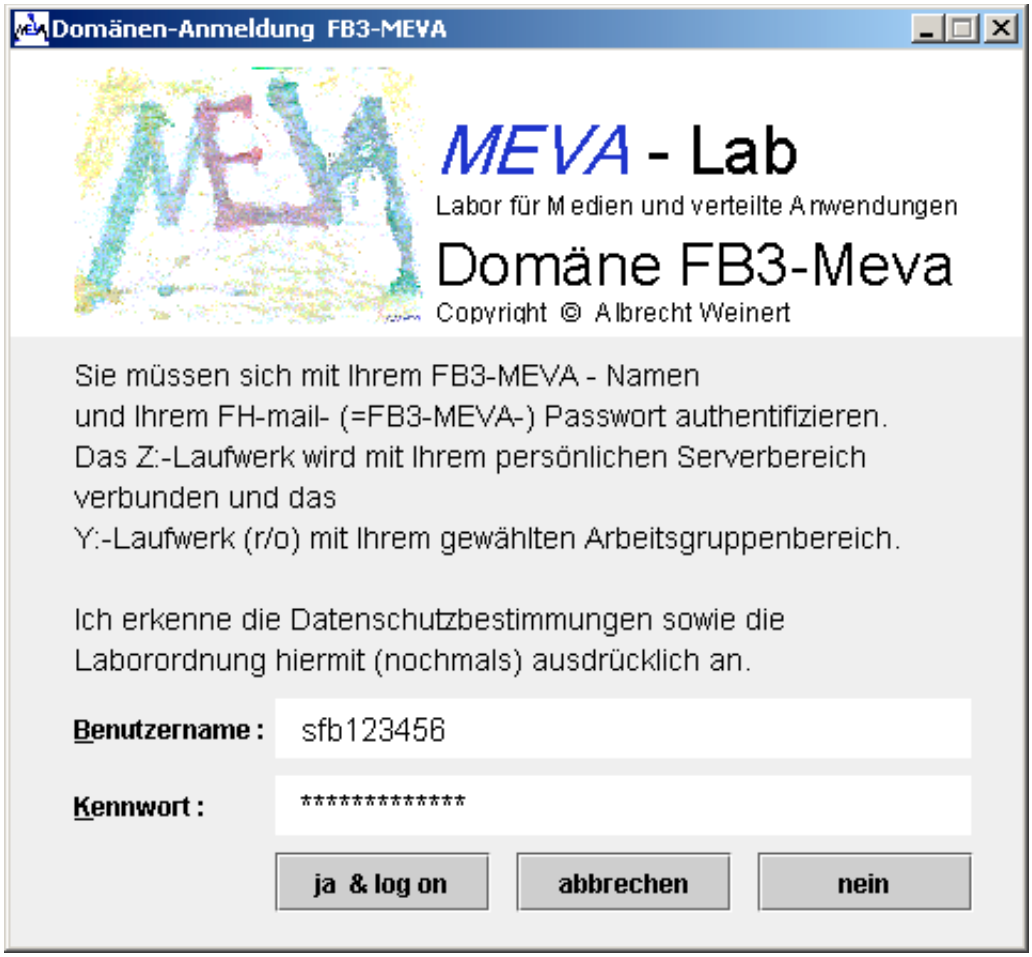

Bild 7: Individuelle Authentifizierung mit LogAlert.java (vgl. Listing 12 ab Seite 26)

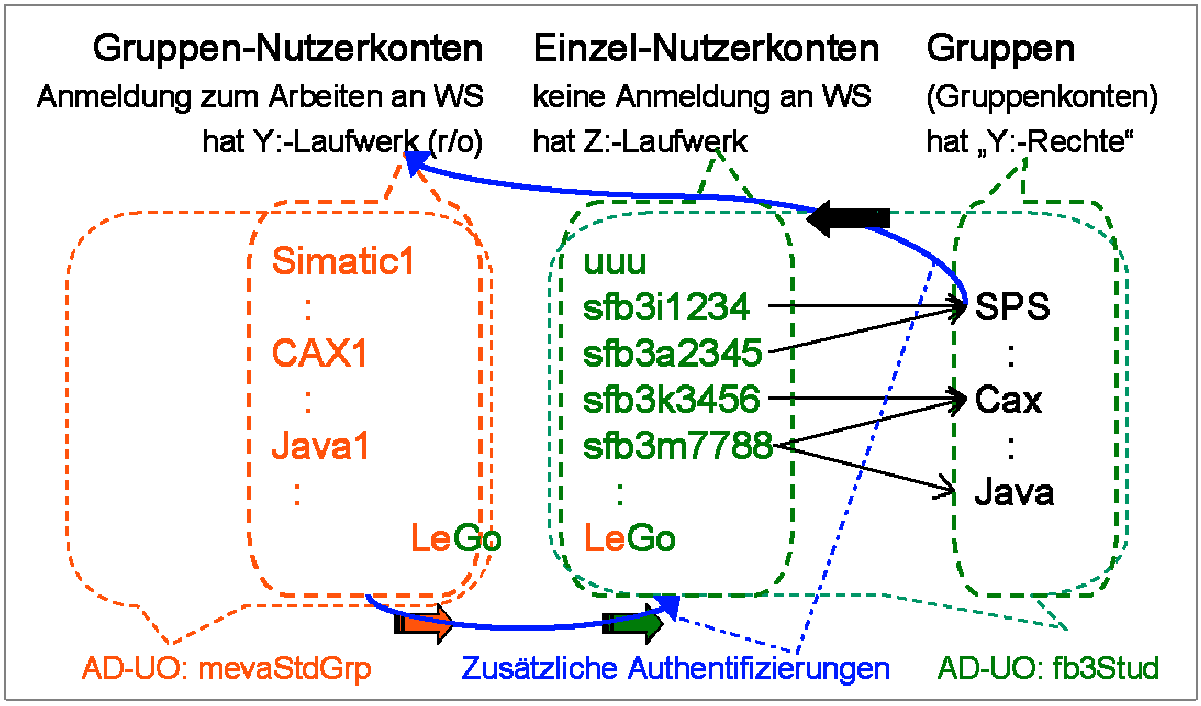

Bild 8: Zur Authentifizierung studentischer Nutzer.

Für die (36) Schulungsrechner (Typ1) gilt folgendes:

- Betriebssystem wird Windows Server 2003 standard edition (W2K3)
- Anmeldeskripte laufen „synchron“ (WS-Registry-Einstellung).
  Das heißt, dass der sich an der WS anmeldende Nutzer nichts tun kann, bevor das Anmeldeskript fertig ist.
- Lokal installiert werden:
  - Java (1.4.2_09) mit framework (als Standard Java-Umgebung im PATH)
  - Java (1.5.0_04) mit framework
  - MS-Office (2000)
  - Star-Office (7 mit update 4)
  - Sophos
  - Eclipse (3.1)
  - Subversion
  - AutoCad
  - EPlan
  - Matlab
  - S7-Projektierung
  - WinCC
  - LabView
  - div. Hilfsprogramme (EditPad, 86x86-Assembler, etc.)
- Die Installation wird über Partitions-Images gesichert und über alle WS des selben Typs verbreitet.
- Die Schulungsrechner und die Laborrechner für studentische Arbeiten kommen in eine eigene OU (caxLabWS) ohne spezielle Gruppenrichtlinien.
- Für die Anmelde-Gruppenkonten wird auf den Schulungsrechnern der „shut down“-Bildschirmschoner installiert und eingestellt (10 Minuten Inaktivität ⇒ Gute-Nacht-Gruß ⇒ Aus in 40 s).

Die geforderte zentrale Schaltung des Internetzugangs für die Workstations wurde zunächst über ein Alias im DNS der Domäne FB3-MEVA geregelt, das bei den Gruppennutzer-Profilen als Internet-Proxy konfiguriert wird. Mit dem Umkonfigurieren des Alias-Eintrags lässt sich der Internetzugang nach außen unterbinden bzw. wieder einschalten. Dies Verfahren wird durch eine automatische Proxy-Konfiguration mit zentral auswechselbaren Konfigurationsdateien (proxy.pac) in einem r/o-Netzlaufwerk (Y:, siehe oben) ersetzt werden.

3.2 Einzelheiten

3.2.1 Windows Server 2003 standard edition

Ein Server-Betriebssystem für studentische Schulungsrechner einzusetzen, scheint auf den ersten Blick ungewöhnlich — und auf den zweiten unnötig und teuer.

Von den Preisüberlegungen bei einzelnen Installationen ist der Fachbereich Informatik dank einer günstigen, von Prof. Dr. Wollert geschlossenen und betreuten Lizenzvereinbarung mit Microsoft glücklicherweise befreit. Da dieser Punkt entfällt und nachdem getestet war, dass man auch von anderen Kollegen geforderte aber unbetreute und ungepflegte Legacy-Anwendungen (Simatic-PG) zum Laufen bringt, blieben für die Entscheidung zugunsten W2K3 (statt XP oder 2K) nur noch Vorteile.

Unter vielen anderen sind dies:

- modernstes MS-Betriebsystem

- beste Ausstattung mit tools zur Unterstützung und Automatisierung der Administrierung,
- professionelles (weitgehend) look and feel schon in den default-Einstellungen,
- weitergehende Berücksichtigung von Sicherheitsanforderungen schon in den default-Einstellungen.

Hier unterscheidet sich W2K3 sehr positiv vor Allem von XP, bei dessen Entwicklung und Grundeinstellung graphischer Schnickschnack die höchste Priorität hatte. Gerade in der FH-Informatikausbildung sollte aber ein professionelles, industrienahes Arbeiten vorgeführt werden können.

3.2.2 Konten und Anmeldung

Wie schon in 3.1 ab Seite 15 dargelegt, gibt es (grob) drei Sorten Benutzerkonten

- privilegierte Konten, also Dozenten, Mitarbeiter („Kernteam“) und FB3-Angehörige etc. (ca. 50 Konten)
- studentische Nutzergruppenkonten (ca. 5 Konten; quasi öffentliche Passworte)
- studentische Einzelnutzerkonten (ca. 1600 Konten; Stand Januar 2006)

Benutzer des ersten Typs sind „landläufige“ Domänenbenutzer mit recht unterschiedlichen Ausprägungen bezüglich Rechten, Profilen und Ressourcenausstattung (von Administrator bis „Gast“).

Der dritte Typ darf sich nie direkt zum Arbeiten an einer Workstation anmelden.

Der zweite Typ darf sich nur bei bestimmten Workstations und unter zusätzlicher Authentifizierung durch ein Konto des dritten Typs anmelden.

Umgekehrt ausgedrückt kann sich ein Nutzer des dritten Typs (studentischer Einzelnutzer) nur über eines der Konten des zweiten Typs anmelden. Dieses Recht (und andere) kann über Gruppenzugehörigkeiten des studentischen Einzelkontos ganz feingranular gemanagt werden.

Namen und Passworte der studentischen Benutzerkonten werden mit den zur selben Person gehörenden FH-email-account und Passwort gleichgehalten. Mit dieser Authentifizierung kann der Studierende neben dem email-Dienst, den FB3-MEVA-Diensten und der FB3-Praktikumsorganisation auch andere FH-weite Dienste in Anspruch nehmen, teilweise auch von außerhalb der FH aus.

3.2.3 Verhindern von Anmeldung, Abmelden

Die Anmeldung eines studentischen Einzelnutzerkontos an einer Labor-Workstation erfolgt (Stand 10.2005) in folgenden Schritten:

- Windowsanmeldung mit einem der (wenigen) Nutzergruppenkonten (cax1 z.B.)
- Abfrage eines dem FH-email-Konto entsprechenden Einzelkontos (sfb3i007 z.B.) und Passworts. (Dies und das meiste Folgendes geschieht mit der Anwendung LogAlert.java.)
- Authentifizieren des Namen-/Passwort-Paares beim zentralen LDAP-Server (der FH).
  Ein Misslingen dieser LDAP-Authentifizierung bedeutet keine direkte Ablehnung; dies geschieht aber ggf. indirekt in den folgenden Schritten.
  (Diese Barmherzigkeit könnte „ungeLDAPte“ Konten dulden, falls man solche zulassen wollte. Sinn ist hier aber lediglich das Tolerieren kurzzeitige Ausfälle des LDAP-Servers oder der Verbindung dorthin.)
- Nötigenfalls Synchronisieren des Passworts des domain-Kontos mit dem gleichnamigen LDAP-Konto. Zentrales Loggen des Anmeldeversuchs.
  (Beides geschieht durch die Anwendung LogServer.java auf einem der DC).
- Authentifiziert durch Einzelkonto (sfb3i007 z.B.) Verbindung mit dem individuellen Fileserver-Bereich (Z:-Laufwerk, \\freigabe\sfb3i007\ im Beispiel).
  Für diesen Bereich hat das Einzelkonto (im Wesentlichen) Vollzugriff.
  Dieser Schritt misslingt, wenn das zum Einzelkonto angegebene Passwort falsch war, sprich nicht mit dem aktuellen zentralen FH-email-Passwort übereinstimmt.
  Dieser Schritt misslingt ebenfalls, wenn das (domain-) Einzelkonto gesperrt ist (total oder zeitgesteuert).
  Er misslingt auch, wenn Java, das Framework (de.a_weinert..) oder eines der verwendeten Java-Tools auf der verwendeten Workstation nicht richtig installiert ist.

Und schließlich misslingt dieser Schritt auch, falls eine durch zwischenzeitliche Änderung nötige Passwortsynchronisierung im vorangegangenen Schritt nicht möglich war.

- Authentifiziert durch Einzelkonto (sfb3i007 z.B.) Verbindung mit dem Gruppen-Fileserver-Bereich (Y:-Laufwerk, \\freigabe\cax1\ im Beispiel).
  Für diesen Bereich hat eine Gruppe (Cax im Beispiel) Lese- und Ausführungsrecht.
  Dieser Schritt misslingt, wenn das Einzelkonto nicht Mitglied der betreffenden Gruppe ist.
  Diese Gruppenmitgliedschaft (Cax im Beispiel) ist praktisch das Privileg, sich via cax1 (im Beispiel) anzumelden.
- Suchen des Namens der Anmelde-Workstation (Computer-Name; PD3W55 z.B.)
  in einer Liste (r/o) im Gruppen-Fileserver-Bereich (Y:-Laufwerk).
  Diese Liste führt diejenigen Rechner auf, an denen sich das Nutzergruppenkonto (cax1\ im Beispiel) anmelden darf.
  Dieser Schritt misslingt, wenn die verwendete Workstation nicht aufgeführt ist.

Ein Misserfolg in irgendeinem der Schritte (Ausnahme LDAP; sie wirkt ggf. wie beschrieben nur indirekt) beendet den Anmeldevorgang durch sofortige Zwangsabmeldung. Durch entsprechende Einstellungen, Anmeldeskripts und Tools wird ein „zwischendurch Herausmogeln“ und Arbeiten mit nur der (quasi öffentlich zugänglichen) Gruppennutzer-Authentifizierung verhindert. Entscheidend dabei ist das sogenannte „synchrone“ Laufen des Anmeldeskripts (vgl. auch Listing 12, ab Seite 26) durch den Registry-Eintrag

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\
DWORD RunLogonScriptSync = 1

und das Verhindern einer Anmeldung bei unerreichbaren DCn durch den Registry-Eintrag

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
DWORD CachedLogonsCount = 0

Dieser Registry-Einträge sind auf allen (!) erlaubten (vgl. auch Listing 15, ab Seite 29) Workstations zu setzen.

Im Profil aller Gruppennutzer ist der “log off screensaver” (10 Minuten Inaktivität, 30 s Warnzeit) eingerichtet. Eine einschlafende Sitzung wird also innerhalb kurzer Warnzeit zwangsabgemeldet, obgleich dies dem unaufmerksamen Nutzer schaden kann. Diese Einstellung ist dennoch zum Schutz der individuellen (Einzel-) Nutzerdaten (des sfb3i007 im obigen Beispiel) notwendig, da ein passwortbewehrter Bildschirmschoner hier nur den Gruppennutzer (cax1 im obigen Beispiel) schützen würde und somit nichts brächte.

Der “log off screensaver” (winexit.scr) funktioniert wegen eines (uralten) Bugs allerdings nur, wenn für den Registry-Eintrag

HKEY_Local_Machine\Software\Microsoft\Windows NT\CurrentVersion\IniFileMapping\Control.ini

jedem das Recht zum „Werte Ändern“ und „Schlüssel Erzeugen“ gewährt wird. Dies kann von Hand mit regedt32 geschehen oder mit einem Grundeinstellungsscript; vgl. Listing 15 auf Seite 29.

3.2.4 File Server und andere Ressourcen für die Nutzer .

Wie im letzten Kapitel schon teilweise beschrieben, hat der erfolgreich angemeldete (studentische Nutzer) drei Dateibereiche:

- “sein” Z:-Laufwerk, \\freigabe\einzelnutzer\; Vollzugriff
- Gruppen Y:-Laufwerk, \\freigabe\gruppenkonto\; Lesen Ausführen
- allgemeines P:-Laufwerk, selten genutzte Programme und Dokumente; Lesen Ausführen

Auf dem Z:-Laufwerk wird dem Benutzer ursprünglich eine Verzeichnisstruktur und Dateien als Muster (einschließlich eines Eclipse-Testprojekts) vorgegeben. Diese sind durch mindere Rechte nur teilweise geschützt. Es liegt im Interesse des Nutzers die (keineswegs einengende) Grundstruktur intakt zu halten, da einige Programme so installiert sind, dass sie ihre Arbeits- und Konfigurationsbereiche „unterhalb Z:“ haben. So ist gewährleistet, dass der individuelle Nutzer seine Anwendungsdaten und teilweise auch -konfigurationen von WS zu WS mitnimmt.

Auf dem (Server-) Laufwerk mit diesen Z:-Freigaben, sind sogenannte Quota, sprich Maxima für die Plattenplatznutzung, eingerichtet. Die Dateigrößensummierung erfolgt pro Dateibesitzer, und dieser ist für neu erstellte Dateien durch das im letzten Kapitel beschriebene Anmeldeverfahren auf der Z:-

Freigabe der hier für die Authentifizierung verwendete Einzelnutzer (also sfb3i007 im dortigen Beispiel) und nicht der für die Workstation-Anmeldung verwendete Gruppennutzer (cax1 im dortigen Beispiel). Diese Maßnahme hält gelegentliche „Filmsaugende“ möglicherweise von ihrem bösen Tun ab; sie verhindert aber zumindest, dass Einzelne missbräuchlich Anderen das Arbeiten mit den Fileserver-Bereichen einschränken.

3.2.5 Druckdienst für Lehrzwecke

Drucken können studentische Nutzer über einen von FB3-MEVA-Druckserver vermittelten Dokumentserver auf einem Nashuatec-Kopierer (DSm627) im Flur vor dem Schulungsraum. Die zu druckenden Dokumente müssen individuell gekennzeichnet werden und können mit einer vierstelleigen Kennung (einigermaßen) vor „Raubdruckern“ geschützt werden. Die so erstellte Druckseite kostet genauso viel wie eine Kopieseite auf dem Gerät.

Anderen (privilegierteren) Nutzern stehen natürlich die übrigen Drucker des MEVA-Lab bzw. der Domäne direkt zur Verfügung. Mit der unkontrollierten und „kostenungebremsten“ Breitstellung von Druckmöglichkeiten für studentische Nutzerkonten aus ziemlich öffentlichen Schulungsräumen wurden in der Vergangenheit leider nicht nur gute Erfahrungen gemacht — gelinde gesagt.

3.2.6 Administrativen Aufgaben, Automatisierung

Eine der ersten Bequemlichkeiten, die eingerichtet wurden, war das Fernein- und Fernausschalten aller Labor-WS; siehe Listing 17 auf Seite 30. Dies funktioniert so nur mit der shutdown.exe von W2K3 (tool kit), die man aber auch auf W2K-Rechnern (z.B. unter C:\programme\util\) verbreiten kann.

Die Skripte zum Einrichten eines Labor-WS-Kontos und eines studentischen Einzelnutzerkontos siehe im selben Kapitel des Anhangs.

4 Betriebserfahrungen

Die Umstellung der Domäne FB3-MEVA auf W2K3-DCs war für die meisten Client-Rechner und andere Server weitgehend unsichtbar. Probleme waren meist auf DNS-Konfigurationsprobleme oder -fehler zurückzuführen. Sie konnten behoben werden. Hier bleibt bis jetzt nur eine Affäre mit einer Büro-WS, die sich eine Hauptsuchdienst-Rolle anmaßt. Dies im konkreten Fall (trotz Einholen von Microsoft TechNet-intergrundinfos) noch nicht (Stand 10.2005) ganz geklärt.

Ferner gab es (unberechtigte) Lizenzprobleme bei Terminalerver-Nutzern, die mit der Installation von W2K3-ServicePack 1auf den betreffenden Servern entstehen. Diese lassen sich durch „händisches“ Neukonfigurieren der Lizenzserver-Informationen unter jeweils gleichen Umständen nur teilweise Beheben (also noch unverstanden).

Ein Labtop-Domänenmitglied (mindestens eines) wurde ohne sonstige Änderung an diesem PC also nur durch Umstellung der Domäne auf W2K3 in seinem Anmelde- und SMB-Verhalten so verdorben, dass er seitdem die externe Arbeit in einem Firmennetz bestreikt.

Inzwischen (22.10.2005) ist für 50 Labor-PC-Konten, ca. 1300 Nutzerkonten mit zwei Gruppenanmeldekonten der Lehr- und Praktikumsbetrieb angelaufen. Anmeldung, Passwortsynchronisierung, Fileserver-Bereiche und für die Lehre eingesetzte Standardsoftware (Java, Eclipse, Office usw.) funktionieren im Wesentlichen erwartungsgemäß und einwandfrei.

Als störanfällig und Störungen auslösend fiel Anwendungs-Software mit Lizenz- und Serveranforderungen auf, die (trotz jeweils korrekt erworbener Lizenzen) nicht zu einem solchen Lehrbetrieb passend gemacht werden kann, wie u.A. AutoCad und EPlan. Hier müssen Alternativen gefunden werden.

5 Appendix

5.1 Skripte, Listings

In diesem Kapitel sind für an diesen technischen Einzelheiten Interessierte einige der wesentlichen Skripte und Konfigurationsdateien aufgeführt. Im laufenden Text wird, um den Textzusammenhalt im jeweils betreffenden Kapitel nicht zu stören, jeweils nur hierher verwiesen.

Voraussetzungen:
Um sofortige Enttäuschungen (bei copy and try) zu vermeiden, sei nochmals darauf hingewiesen, dass von dem Folgenden das weitaus Meiste ohne korrekte Java- und meist auch Framework-Installation (de.a_weinert..) fast nichts läuft. Teilweise sind über die Windows-Grundinstallation hinaus auch Werkzeuge aus den Admin- bzw. Resource tool kits erforderlich.

Die Anwendung setACL.exe ist (geniale) freeware.
Der Virenscanner Sophos steht durch eine FH-Lizenz zur Verfügung.

Listing 9: Skript klinkVir.bat zur automatischen Sophos-Aktualisierung (läuft auf WSs und DCn)

```
@Echo.
@Echo klinkVir.bat V01.04 (05.05.2005) (c) A. Weinert
@REM  Win32 - Batch - Datei; kann als automatische Task / als Dienst
@REM  verwendet werden.
@REM  setzt Java (JDK >= 1.4.x) erweitert um Framework de.a_weinert...
@REM  (aWeinertBib.jar vom 04.05.2005 oder jünger) voraus.
c:
md \temp\vir\angee
cd \temp\vir
java Del -empty angee\

@if NOT "%sophosDir%X" == "X" goto :sophDset
set sophosDir=%ProgramFiles%\Sophos SWEEP for NT
:sophDset

@if NOT %sophosSrc%X == X goto :sophSset
if not exist \\Pd310s\vir\angz.zip goto :sophSvar2
if not exist \\Pd310s\vir\web_ides.zip goto :sophSvar2
set sophosSrc=\\Pd310s\vir\
goto :sophSset

:sophSvar2
set sophosSrc=http://service.fh-bochum.de/
:sophSset

@Echo.
@Echo Aufdaten des Sophos-Dienstes (von %sophosSrc%
@Echo           nach %sophosDir%)
@Echo.

java UCopy -np %sophosSrc%angz.zip -u angz.zip
if ERRORLEVEL 2 goto :noAngeeError
if ERRORLEVEL 1 goto :noAngee
:angeeDa
@echo Neue Installationsdatei  angz.zip geholt.
@java de.a_weinert.apps.FS .\angz.zip -o -log angeeDate.txt
```

```
cd angee
jar xvf ..\angz.zip
@Echo Sophos Installation / Update wird gestartet.
@Echo.
setup.exe -ni
cd ..
@REM Näheres mit java AskAlert -? bzw. java UCopy -?
@REM -mx.Paus. 120s -2Knöpfe "W" "A" -timeout wie Ja/Weiter Mld Frg Tit
java AskAlert -w 1200 -2bpc -tDy "Sophos Installation / Update" "Weiter,
wenn fertig" "Sophos Installation"

if ERRORLEVEL 1 goto :ende
goto :noAngee

:noAngeeError
@echo Fehler beim Holen von angz.zip
:noAngee

:ides
java UCopy -np %sophosSrc%web_ides.zip -u web_ides.zip
@if ERRORLEVEL 2 goto :noIdesError
@if ERRORLEVEL 1 goto :noIdes

:idesDa
@echo Neue Informationsdatei  web_ides.zip geholt.
@java de.a_weinert.apps.FS .\web_ides.zip -o -log idesDate.txt

cd /D %sophosDir%
jar xfv  C:\temp\vir\web_ides.zip
net stop  SWEEPSRV.SYS
net start SWEEPSRV.SYS
goto :noIdes

:noIdesError
@echo Fehler beim Holen von web_ides.zip
:noIdes

:ende
@Echo.
```

Listing 9 Ende: Skript klinkVir.bat zur automatischen Sophos-Aktualisierung

Listing 10: Properties-Datei WichtelBackup.properties für Anwenderdaten-Backup (für FileSevices.java)

```
#  Property-File für FileServices.java als Backup-Server
#  WichtelBackup.properties V00.03, 18.05.2005, 22.08.2005

# Achtung Spezial-Belegung word0..2
word-0=logDat

# Wiederholung:  normal alle 24h um 02:17;  schnell ohne Log (n.benutzt)
rate=       -1
atHour=     02
atMinute=   17
fastRate=   60
fastSilent= true
```

```
#Aufdat-Default-Optionen
types=+.+
recursion= true
days=      nosetting
difOld=    120000
zoneSafe=  true
lcNames=   false
noNew=     false
noMd=      false
delEmpty=  false
dirCritWild=
dirCritOmit=
noClean=   true

#Dienst 0 (\\Pd323s\home\meier Siemens BDC)
qvz0=\\\\Pd323s\\home\\meier\\
zvz0=D:\\home\\meier\\
bvz0=D:\\home\\meier-1\\

#Dienst 1 (\\Pd324s\home\weinert primary DC)
qvz1=\\\\Pd324s\\home\\weinert\\
zvz1=D:\\home\\meier\\
bvz1=D:\\home\\meier-1\\

#Dienst 2 (\\Pd323s\home\schulze Siemens BDC) ....
qvz2=\\\\Pd323s\\home\\schulze\\
zvz2=D:\\home\\schulze\\
bvz2=D:\\home\\schulze-1\\

#Dienst 3 (\\Pd324s\home\schulze primary DC)
qvz3=\\\\Pd324s\\home\\schulze\\
zvz3=D:\\home\\schulze\\
bvz3=D:\\home\\schulze-1\\

#Dienst 10 (\\Pd310s\FB3WWW\AktuellerStand   Wichtel)
qvz10=\\\\Pd310s\\FB3WWW\\AktuellerStand\\
zvz10=D:\\FB3WWW\\AktuellerStand\\
bvz10=D:\\FB3WWW\\WWWBack\\

#Dienst 11 (\\Pd310s\FB3WWW\Infos   Wichtel)
qvz11=\\\\Pd310s\\FB3WWW\\Infos\\
zvz11=D:\\FB3WWW\\Infos\\
bvz11=D:\\FB3WWW\\Infos-1\\
```

Listing 10 Ende: Properties-Datei WichtelBackup.properties für Anwenderdaten-Backup (gekürzt und Namen etc. teilweise geändert)

Listing 11: Skript homeAnm.bat zum Log-In für privilegierte Benutzer

```
@Echo.
@Echo AnmeldeScript homeAnm.bat  f. home/%USERNAME%  Start
@Echo.
@Echo zuletzt modifiziert am 25.08.2005 16:08 auf PD324S von A. Weinert
@Echo wg.Umstell.d. Domain FB3-MEVA auf W2003 Srv (PD324S, .23S, (.21S))
@Echo.
@Echo.
```

```
net use p:   /delete
net use z:   /delete

net use p:    \\PD324S\Programme /persistent:no
if errorlevel 1 goto :noserver
net use z:    \\PD324S\home     /persistent:no
if errorlevel 1 goto :noserver

@echo Der Server PD324S ist erreichbar.
@net time /domain:fb3-meva /set /yes
@echo off
goto :look1

:noserver
net use p:   /delete
net use z:   /delete

@echo.
@Echo Der FB3-MEVA - Server PD324S ist nicht zu erreichen.
@Echo Der Server PD323S wird ersatzweise benutzt (Z: und P:).
@echo.
@Echo Hinweise:
@Echo 1.) Sie haben evtl. nicht alle Programme zur Verfuegung.
@Echo 2.) Achten Sie ggf. auf Konsistenzprobleme bei Z: = home PD2323S !=
PD324S
@echo.

net use p:    \\PD323S\Programme /persistent:no
net use z:    \\PD323S\home     /persistent:no
@echo off

:look1

REM change         v    this                    v signature to force
firsttime start
set anmeldSignature=%USERNAME%homeAnm.bat07.12.04
if not exist %SystemDrive%\config\%USERNAME%First.log  goto :firsttime
findstr %anmeldSignature% %SystemDrive%\config\%USERNAME%First.log
if not errorlevel 1 goto :ende

:firsttime

md %SystemDrive%\config
@Echo %anmeldSignature% > %SystemDrive%\config\%USERNAME%First.log

@echo.
@Echo on
reg import editpadcuruserreg.reg
@Echo off

@REM weitere "firsttime preps" für home-Benutzer hierher

@echo.
@Echo ***  Welcome home/%USERNAME% for the first time on this PC.
@Echo ***  Willkommen, home/%USERNAME%, beim ersten Mal auf diesem
Computer.
goto :stopp
```

```
:ende
@echo.
@Echo ***  Welcome  again on this PC ! home / %USERNAME%
@Echo ***  Erneut Willkommen, home / %USERNAME%.
:stopp
@Echo Press any Key or close this window.
@Echo Bitte Tasteneingabe oder Fenster zu.
@echo.
@Echo AnmeldeScript (25.08.2005, PD324S.sysvol) f. %USERNAME%  Ende
@set anmeldSignature=
@pause
```

Listing 11 Ende: Skript homeAnm.bat zur Anmeldung privilegierter Nutzer

Listing 12: Anmeldeskript studGrup1Anm.bat zur zusätzlichen individuellen Authentifizierung bei „Sammelkonto“-Anmeldung

```
@Echo.
@Echo AnmeldeSkript studGrup1Anm.bat  f. Studierendengruppe  %USERNAME%
@Echo Zuletzt modifiziert am 03.10.2005, 17:21, von Albrecht Weinert
@Echo.
@Echo Einzel-Authentifizierung %USERNAME% am PC %COMPUTERNAME%:
@Echo.

@C:\Programme\jdk\bin\java.exe -jar C:\Programme\util\LogAlert.jar  Z:
               \\193.175.113.245\fb3stud\
@if NOT ERRORLEVEL 4  goto :connectP

:chassDeGickel
@shutdown /l
@Echo.
@Echo Keine solche Anmeldung als %USERNAME% am PC %COMPUTERNAME%.
@Echo.
goto :stopp

:connectP
net use P: \\PD322S\ProgServer  /PERSISTENT:NO
@echo.

@REM change         v    this    v signature to force firsttime start
set anmeldSignature=%USERNAME%studGrup1AnmBat_%USERNAME%
if not exist %SystemDrive%\config\%USERNAME%First.log  goto :firsttime
findstr %anmeldSignature% %SystemDrive%\config\%USERNAME%First.log
if not errorlevel 1 goto :ende

:firsttime
@md %SystemDrive%\config
reg import editpadcuruserreg.reg
@Echo %anmeldSignature% > %SystemDrive%\config\%USERNAME%First.log
@echo.
@Echo ***  Zum ersten Mal Willkommen, mevaStGrp/%USERNAME%.
goto :stop

:ende
@echo.
@Echo ***  Erneut Willkommen, fb3Stud/%USERNAME% am PC %COMPUTERNAME%.
```

```
:stopp
@echo.
@Echo AnmeldeScript (12.09.2005, PD322S.sysvol) f. %USERNAME%  Ende
@set anmeldSignature=
```

Listing 12 Ende: Anmeldeskript studGrup1Anm.bat

Hinweis: Die Anwendung LogAlert (.java) loggt bei entsprechenden Eingaben oder Misslingen der Aktionen — wie Laufwerk verbinden etc. — ggf. selbst den Benutzer aus.

Listing 13: Administratorskript PD3join.bat (Parameter Namensergänzung zu PD3...)
Hinzufügen einer Schulungs-Workstation zur Domäne FB3-MEVA,
ou= caxLabWS mit nötigenfalls Erzeugen des Computerkontos.

```
@echo .
@echo PD3join.bat V0.00 (21.10.2005 13:14) A. weinert
@echo .
@echo Pd3join PD3-WS-Bezeichnung (ohne PD3) Raum (D3-08 z.B.)
"Beschreibung"
@echo Pd3join PD3%1 %2   "%~3"
@echo.
@if not %3x==x goto :make
@echo Parameterfehler!
@echo Aufrufbeispiel:
@echo    Pd3join W01 D3-13 "CaxLab -Workstation (Typ 1)"
goto :stopp

:make
net computer \\PD3%1 /add
@echo.
dsmove "CN=PD3%1,CN=Computers,DC=FB3-MEVA,DC=fh-bochum,DC=de" -newparent
OU=caxLabWS,DC=FB3-MEVA,DC=fh-bochum,DC=de
@echo.
dsmove "CN=PD3%1,OU=SchrottKonten,DC=FB3-MEVA,DC=fh-bochum,DC=de" -
newparent OU=caxLabWS,DC=FB3-MEVA,DC=fh-bochum,DC=de

netdom ADD PD3%1 /DOMAIN:FB3-MEVA
                 /OU:OU=caxLabWS,DC=FB3-MEVA,DC=fh-bochum,DC=de
dsmod computer "CN=PD3%1,OU=caxLabWS,DC=FB3-MEVA,DC=fh-bochum,DC=de"
                 -loc %2 -desc "%~3"

netdom join PD3%1 /DOMAIN:FB3-MEVA /UserD:admin /PasswordD:*
           /UserO:administrator /PasswordO:metsys2005 /REBoot
                    /OU:OU=caxLabWS,DC=FB3-MEVA,DC=fh-bochum,DC=de

:stopp
@echo.
```

Listing 13 Ende: Administratorskript PD3join.bat

Hinweis: Das zweimalige dsmove holt das Computerkonto sowohl aus Computers (neu entstanden) als ggf. auch aus Schrottkonten (recycling). Beide Anweisungen stehen so „blind“ hintereinander, da dsmove (fast möchte man sagen Microsoft-üblich) keine verwertbaren return-Codes liefert.

Listing 14: Administratorskript makeStudUser.bat
Erzeugen eines studentischen Einzelkontos (läuft auf PD322S).

```
@echo.
@REM Studentischen Benutzer %1  in  ou fb3stud erzeugen
@Echo.
@Echo V 00.03, 18.10.2005 10:37) : setzt Standardgruppe Cax
@echo.
@echo.
@Echo make user %1 %1 %2  %3 %4  %5 %6 %7 .. %9

if not %9x==x goto :parsDa

@Echo Aufruf
@Echo  makeStudUser name passw Vorn Nachn  Abt=StdRi PLZ Ort Sem=Pos  email
@Echo  // Batch-File  par1 par2  par3 par4    par5  par6 par7    par8  par9
@echo.
@Echo Beispiel:
@Echo    makeStudUser sfb3i007 canKill James Bond I  W44801C Kensington 11
@Echo                                              james.bond@fh-bochum.de
goto :stopp

:parsDa

@echo.
net user %1 %2 /ADD  /COMMENT:"stud. Benutzer"
          /SCRIPTPATH:unberAnm.bat  /FULLNAME:"%~4, %~3" /DOMAIN
@echo.
@echo.

dsmove "CN=%1,CN=Users,DC=FB3-MEVA,DC=fh-bochum,DC=de"
           -newparent OU=fb3Stud,DC=FB3-MEVA,DC=fh-bochum,DC=de
net group cax %1 /add
@echo.

:dsMod
@echo.
dsmod user "CN=%1,OU=fb3Stud,DC=FB3-MEVA,DC=fh-bochum,DC=de"
                  -fn %3 -ln %4 -display %1 -title %8 -dept %5
                         -company "FB3 MEVA-Lab"  -email %9

@echo.
@echo ------------------------------------------------------
@echo.

robocopy G:\fb3stud\z-muster    G:\fb3stud\%1\
                        /S /E /SEC /A-:RASH /R:4 /W:6

setacl G:\fb3stud\%1   /dir  /grant %1 /full /P:no_copy
setacl G:\fb3stud\%1  /dir  /revoke  Benutzer /list_dir
setacl G:\fb3stud\%1  /dir  /revoke  Benutzer /read
setacl G:\fb3stud\%1  /dir  /revoke  Benutzer /read_ex
setacl G:\fb3stud\%1  /dir  /revoke  Benutzer /full

:stopp
@Echo.
```

Listing 14 Ende: Administratorskript makeStudUser.bat

Listing 15: Administratorskript baseInst1.bat; Diverse Grundeinstellungen für eine Labor-Workstation PD3xyz (xyz = %1 = Parameter1; läuft auf PD322S).

```
@echo.
@echo baseInst1.bat V0.00 (22.10.2005 16:14) A. Weinert
@echo.
@echo baseInst1 PD3-WS-Bezeichnung (ohne PD3)
@echo baseInst1 PD3%1
@echo.
@if not %1x==x goto :make
@echo Parameterfehler!
@echo Aufrufbeispiel:
@echo         baseInst1  150
goto :stopp

:make
goto  :phase2Test

call makeUserReadableDir.bat  \\PD3%1\C$\bat
robocopy C:\c-Laufwerk\bat    \\PD3%1\C$\bat\   /S /E  /R:4 /W:6 /NP

md \\PD3%1\D$\temp
setacl  \\PD3%1\D$\temp   /dir  /grant  Jeder   /full /P:no_dont_copy
md \\PD3%1\D$\tmp
setacl  \\PD3%1\D$\tmp   /dir  /grant  Jeder   /full /P:no_dont_copy
md \\PD3%1\C$\temp
setacl  \\PD3%1\C$\temp   /dir  /grant  Jeder   /full /P:no_dont_copy
call makeUserReadableDir.bat  \\PD3%1\C$\temp\vir

call makeUserReadableDir.bat      \\PD3%1\C$\programme\util
call makeUserReadableDir.bat      \\PD3%1\C$\programme\packedVersions
call makeUserReadableDir.bat      \\PD3%1\C$\programme\jdk
md         \\PD3%1\C$\programme\jdk\bin
md         \\PD3%1\C$\programme\jdk\docs
Compact /C  \\PD3%1\C$\programme\jdk\docs

robocopy C:\c-Laufwerk\programme\
               \\PD3%1\C$\programme\  /S /E  /R:4 /W:6 /NP

xcopy  /y  C:\C-Laufwerk\programme\packedVersions\winexit.scr
                                 \\PD3%1\C$\windows\system32\

reg add
\\PD3%1\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\
                 /v RunLogonScriptSync /t REG_DWORD /d 1 /f
reg add
  "\\PD3%1\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\"
               /v CachedLogonsCount" /t REG_DWORD /d 0 /f

setacl
  "\\PD3%1\MACHINE\Software\Microsoft\Windows NT\CurrentVersion\IniFileMapping\control.ini"
                     /registry   /grant  Jeder /create_subkey
setacl
  "\\PD3%1\MACHINE\Software\Microsoft\Windows NT\CurrentVersion\IniFileMapping\control.ini"
                     /registry   /grant  Jeder /set_val


:stopp
@Echo.
```

Listing 15 Ende: Administratorskript baseInst1.bat

Listing 16: Hilfsskript makeUserReadableDir.bat
(Domänen-Admin, System: Vollzugriff, Domänen-Benutzer: Lesen, Ausführen)

```
@echo.
@echo makeUserReadableDir.bat (%1)  V0.00 (21.10.2005 15:20) A. Weinert
@echo.
@if not %1x==x goto :make
@echo Parameterfehler!
@echo Aufrufbeispiel:
@echo         makeUserReadableDir  \\PD3Wxyz\C$\bat
@echo.
@Echo Erzeugt angegebenen Verzeichnis mit Domänen-Admins Vollzugriff
@echo und   Domänen-Benutzer Lesen Ausführen Angucken (ohne Erben)
goto :stopp

:make
@chcp 28591
md %1
setacl  %1   /dir  /grant  Domänen-Admins   /full /P:no_dont_copy
setacl  %1   /dir  /grant  SYSTEM    /full
setacl  %1   /dir  /grant  Domänen-Benutzer /read
setacl  %1   /dir  /grant  Domänen-Benutzer /read_ex
setacl  %1   /dir  /grant  Domänen-Benutzer /list_folder
:stopp
@Echo.
```

Listing 16 Ende: Hilfsskript (Prozedur) makeUserReadableDir.bat

Listing 17: Administratorskript CaxWSoff.bat
(caxws.txt ist eine Liste aller dieser WSs)

```
@echo.
@echo Alle CAX Workstations (Liste C:\bat\caxws.txt) aus
@echo.
@echo CAX-WS

FOR /F   "eol=; tokens=1,* "  %%i   in (C:\bat\caxws.txt)
             do call C:\bat\wsOff.bat %%i

@echo.

=======================     CaxWSoff.bat / WSoff.bat    ==============

@echo.
@echo Workstation %1  ausschalten, falls noch an

if %1x==x goto :stopp

java de.a_weinert.apps.PCon %1 -v
@if ERRORLEVEL 5 goto :stopp

shutdown /s /m \\%1 /t 199  /d p:1:1
              /c "Good night, good night, it's time to go to bed"

:stopp
@echo.
```

Listing 17 Ende: Administratorskript caxWSoff.bat + WsOff.bat (die Prozedur)

5.2 Literatur

[Boswell] Boswell, William, Windows Server 2003 für Insider, Markt und Technik 2003

[MS2003] Microsoft Press, Windows Server 2003, Die technische Referenz (6 Bände)

[Fr2005] Frisch, AEleen, und Klein, Helga, Windows Befehle für XP und Server 2003, O'Reilly

Im übrigen wären hier zahllose Dokumente aus dem Internet

- `www.microsoft.com`
- `www.fh-bochum.de/fb3/meva-lab/docu`

und aus anderen Quellen zu nennen; u.A.

[Boy] Boyce, Jim, Comprehend Windows Server 2003 trust relationships and functional levels http://asia.cnet.com/itmanager/netadmin/0,39006400,39172450,00.htm

[MSTN1] Microsoft TechNet,
Migration von Windows 2000-Domänen auf Windows Server 2003

[MSTN2] Microsoft TechNet, Windows Server 2003 Supported Upgrade Paths

[MSTN3] Microsoft TechNet, Verwaltungsdienste - eine technische Übersicht

[MSTN4] Microsoft TechNet, Koexistenz von Windows Server 2003 und Windows NT 4.0. März 2003

[MSTN5] Microsoft TechNet, Remote Desktop Protocol (RDP) Features and Performance

[MSTN6] Microsoft TechNet, Windows Server 2003-Sicherheitshandbuch

[MSTN7] Microsoft TechNet, Top 10 Features of Windows Server 2003 for Organizations upgrading from Windows NT Server 4.0

[We04_a] Weinert, Albrecht, Zehn Schriite nach Java1.5,
(http://www.fh-bochum.de/fb3/meva-lab/docu/tojava15.pdf)

[We02_b] Weinert, Albrecht, Zur Installation des JDK,
(http://www.fh-bochum.de/fb3/meva-lab/docu/java-install.txt)

[We04_b] Weinert, Albrecht, Tipps zu Sophos Antivirus (nur FH intern),
(http://www.fh-bochum.de/fb3/meva-lab/docu/sophos-install-tipp.txt)

[Stan03d] Stanek, William, Microsoft Windows Server 2003, Taschenratgeber für Administratoren, Microsoft Press Deutschland 2003

[Stan03a] Stanek, William, Microsoft Windows Server 2003, Administrator's pocket consultant, Microsoft Press 2003

[Mac03d] MacKin, J.C., und McLean, Ian, Administrieren einer Microsoft Windows Server 2003 Nrtzwerkinfrastruktur, Microsoft Press Deutschland 2003

5.3 Abkürzungen

A

ACL Access control list

AD Active Directory

APM Advanced Power Management, Stromsparfunktionen

API Programmierschnittstelle zu allgemein verwendbaren Bibliotheken und den Funktionen des Ziel-Betriebssystems (Application Programming Interface)

ARP Address Resolution Protocol (TCP/IP-Protokoll, Übersetzung von IP- in MAC-Adressen)

ASCII	American Standard Code for Information Interchange, Festlegungen einer Kodierung von (Text-) Zeichen
B	
B&B	Bedienen und Beobachten (von Prozessen)
BDC	Backup domain controller
BeSy	Betriebssystem
BIOS	Basic Input/Output System, grundlegende Betriebssystemdienste unter anderem für den Rechnerstart; im Allgemeinen in einem ROM hinterlegt
BO	Bedienoberfläche (=GUI)
BuB	Bedienen und Beobachten (von Prozessen)
C	
C	Programmiersprache (das ist eigentlich keine Abkürzung, sondern ein Durchbuchstabieren von Programmiersprachen: A, B, BCPL,C, ?)
C++	Objektorientierte Weiterentwicklung von C
CAD	Computer aided design
CASE	Computer Aided Software Engineering
CAPI	Common ISDN Application Programming Interface
CAX	Computer aided alles Mögliche; insbesondere das CAX-Labor des FB3 der FH Bochum
CC	Global Catalogue, wesentliches, zentrales AD-Element
CD	Compact Disc, optisches entfernbares Plattenspeichermedium (ca. 800 MByte)
CGI	Common Gateway Interface, Verfahren zur Übertragung von Parametern an HTTP-Server- Programme beziehungsweise -Skripte
CIM	Common Information Model
CORBA	Common Object Request Broker (ORB) Architecture
CPU	Central processing unit; Prozessor
CVS	Concurrent versioning system
D	
DBMS	Datenbankmanagementsystem (database management system)
DC	Domain controller
DCF	DCF77 = Atomzeit-Sender auf 77,5kHz; D: Deutschland, C: Langwelle, F: Frankfurt (genauer Mainflingen bei Frankfurt)
DDL	Data definition language
DES	Data Encryption Standard (der US-Regierung, Exportrestriktion)
DHCP	Dynamic host configuration protocol
DLL	Dynamic Link Library; zur Programmlaufzeit ladbare Bibliothek
DNS	Domain name system
DOS	Disc operating system; Plattenbetriebssystem (oft einschränkend im Sinne MS-DOS verwendet)
DSA	Digital Signature Algorithm, ein (Verschlüsselungs-) Standard der US-Regierung (mit Exportrestriktion)
DTD	Document Type Definition. Eine Metasprache zur Beschreibung von Seitenbeschreibungssprachen wie beispielsweise HTML

DTMF	Desktop management Task force
DV	Datenverarbeitung (=IT)
E	
E/A	Ein- und Ausgabe
EE	Enterprise Edition (Bezeichnung für die Mächtigkeit von SW-Tools)
F	
FAQ	Frequently Asked Questions (Hilfetexte in Frage-Antwort-Form)
FB	Fachbereich; insbesondere Fachbereich Elektrotechnik und Informatik der FH Bochum
FH	Fachhochschule; insbesondere die FH Bochum
FO	Fibre optic (Glasfaser)
FSMO	Flexible single master operation; W2K- / W2K3- (Sonder-) Rollenzuweisung
FTP	File Transfer Protokoll, ein Internet-Protokoll zur Übertragung von (einzelnen unverknüpften) Dateien
G	
GCD	Global catalogue; AD- bzw. LDAP-Funktion
GUI	Graphical User Interface; Graphische Anwenderoberfläche (=BO) Bei Java wird die Erstellung einer GUI mit den Klassen des AWT unterstützt.
GUID	Global unique identifier; Nummer, die einem Nutzer in einem Netz (meist heimlich) zugeordnet wird
H	
HLL	High level language; höhere Programmiersprache
HTML	Hypertext Markup Language. Beschreibungssprache für verknüpfte Seiten, die unter anderem mit HTTP im WWW übertragen werden. Die Beschreibung von HTML ist der RFC 1866.
HTTP	Hypertext Transfer Protokoll. Ein Internet-Protokoll zur Übertragung von WWW-Seiten.
HP	Hewlett Packard (hier i.A. als Rechner- und Peripheriegerätehersteller)
HW	Hardware
I	
ICS	Internet Connection Sharing; MS-NAT
IDE	Integrated development environment; integrierte Entwicklungsumgebung
IDL	Interface Definition Language (insbesondere der OMG)
IE	MS Internet Explorer (Browser mit zusätzlichen und i.A. unsicheren BeSy-Funktionen)
IEC	International Electrotechnical Commission
IMAP v4	Internet Message Access Protocol, version 4
IT	Information Technology (DV)
J	
J2EE	Java 2 Enterprise Edition
JAR	Java Archive; Java-Archiv. Insbesondere zur Zusammenfassung mehrerer zu einer Anwendung oder einem Applet gehörender Klassen- und sonstigen Dateien. Das Dateiformat entspricht .zip. JAR ist auch das JDK-Werkzeug zum Erstellen und Handhaben solcher Archive.
JDBC	Java Database Connectivity (Java Datenbankanschluss)

JDK Java Development Kit; der Werkzeugsatz für die Entwicklung mit Java

JNDI Java Naming and Directory services Interface

JRE Java Runtime Environment; JDK-Subset ohne Entwicklungswerkzeuge, reine Laufzeitumgebung

JSP Java Server Pages

JVM Java virtual machine; der eigens für Java erfundene Prozessor. Er wird im Allgemeinen auf dem jeweiligen Zielsystem emuliert.

L

LAN Local area network; Datennetz für mittlere Entfernungen

LDAP Lightweight Directory Access Protocol

M

MAC Media Access Control (Protokollschicht: HW-Zugriff aufs Netzwerk)

MByte Megabyte, 1024 KByte, also 1024 * 1024 = 2^{20} Byte

MEVA Das MEVA-Lab ist das Labor für Medien und verteilte Anwendungen des Fachbereichs Elektrotechnik und Informatik (FB3) der FH Bochum; der Autor ist Leiter dieses Labors.

MIME Eine Internet-Spezifikation, die das Versenden von binären Dateianhängen mit elektronischer mail beschreibt. (Multipurpose Internet Mail Extensions)

MS Microsoft (bestimmt weitgehend das Marktgeschehen bei PC-Software)

MS-DOS Microsoft Disc operating system; Betriebssystem für PCs

N

NT New Technology (meist synonym für MS-Windows NT)

NT4 Betriebssytem Windows NT Version 4 (i.A. mit Servicepack 6a)

NTFS Windows NT File System

O

ODBC Open Database Connectivity

ODMG Object Database Management Group

OO Objektorientierung, objektorientiert

OOP Objektorientiertes Programmieren

ORB Object request broker

OU Organisation unit, AD-container für Objekte, Ansatzpunkt für Gruppenrichtlinien

P

PC Personal Computer; Persönlicher Rechner. Einengend sind meist Rechner mit Intel-80x86-Architektur und Microsoft-Betriebssystemen — MS-DOS, Windows — gemeint

PDC Primary domain controller

PDF Portable Document Format

PG Programmiergerät, für PLC bzw. SPS

PLC Programmable Logic Controller (umfasst u.A. SPS)

PNG Portable Network Graphic, ein Format für Bilddateien (.png)

POP Post Office Protocol (i.a. mit nachgestellter Versionsnummer: POP3)

R

RAM	Random access memory; Schreib-/ Lesespeicher
RFC	request for comment; Internet-Standards und -Vornormen
RMI	Remote Method Invocation; Aufruf einer Methode auf einem anderen Knoten
r/o	read only; nur Lesezugriff; schreibgeschützt
ROM	Read only memory; Festwertspeicher
RSA	Verschlüsselungsverfahren nach Rivest, Shamir und Adleman

S

SCSI	Small Computer System Interface (parallele Standard-Schnittstelle für Peripherie)
SASL	Simple Authentication and Security Layer (RFC 2222)
SMTP	Simple Mail Transfer Protocol (ein TCP/IP-Protokoll für E-Mail)
SNI	Siemens Nixdorf (Computerhersteller)
SP	Service Pack; Ergänzungs- und Korrekturlieferung zu einem Softwareprodukt
SPS	Speicherprogrammierbare Steuerung, kleines Automatisierungsgerät
SQID	Unix- / Linux-Proxy für http(s) und ftp
SQL	Structured query language, Datenbankbearbeitungssprache
SrvEnt	Server, enterprise edition
SrvStd	Server, standard edition
SSO	Singe sign on, zentrale firmenweite Authentifizierung (speziell MS-SSO-Lösung für W2K3)
SW	Software

T

TC	Technical Committee, Arbeitsgruppe (oft eines Normungsgremiums)
TCP/IP	Transmission control protocol / Internet protocol
TM	Trademark, Geschütztes Warenzeichen (wie zum Beispiel Java™)

U

UCS	Universal Character Set gemäß ISO/IEC 10646, sprich Unicode
UDDI	Universal Description, Discovery and Integration, Schnittstelle zur Registrierung, Beschreibung und zum Suchen von Web Services (auf Basis von XML und SOAP)
UML	Unified Modelling Language; Sprache zur Darstellung von Objektbeziehungen
URL	Uniform resource locator; Adresse einer Datei im Internet
USV	Unterbrechungsfreie Stromversorgung
UTC	coordinated universal time; eine international einheitliche (astronomische) Zeitdefinition
UTF	Unicode Transformation Format
UTF-8	UTF 8-bit encoding form, Serialisierung von Unicodezeichen als Sequenz von 1 bis 4 Bytes
UUID	Universal unique identifier, Nummer, die einem Nutzer in einem Netz (meist heimlich) zugeordnet wird

V

V.24	Serielles Übertragungsprotokoll
VBX	Visual Basic Extensions (Microsoft)

VM	Virtual Machine, gedachte oder simulierte Rechnerarchitektur
W	
W2K	Betriebssytem Windows 2000
W2K3	Betriebssytem Windows 2003
W3	Amerikanische Kurzform für WWW
W3C	WWW-Consortium; Standardisierung der WWW-Verfahren und Protokolle, RFCs
WAN	Wide Area Network (Netzwerk zur Datenübertragung, > 2km)
WBEM	Web based Enterprise Management (DTMF- Initiative)
WMI	Windows management instrumentation (MS - DTMF - Implementierung)
WS	Wokstation, Rechner ohne (primäre) Serverfunktionen; schließt Installation einer Server-Betriebssystemvariante nicht aus
WSUS	Windows Server Update Service (Firmen-Server zum internen Verteilen von MS-Updates)
WWW	World Wide Web, Gesamtheit der HTML-Seiten im Internet
X	
X86	INTEL-80x86-Rechnerarchitektur, binärkompatible Linie von 8086 über 80286, 80386, 80486 bis Pentium.
XML	Extensible mark-up language, erweiterbare Datenbeschreibungssprache
XP	Betriebssytem Windows XP