Albrecht Weinert

Windows Server 2003

Domain FB3-MEVA

IT-Infrastruktur im Firmennetz
Renovierung 2007

Stand: 09.01.2008

MEVA Lab
Medien und verteilte Anwendungen

Albrecht Weinert
Labor für Medien und verteilte Anwendungen (MEVA-Lab)
Fachbereich Informatik der FH Bochum

Renovierung der Domain FB3-MEVA, der IT-Infrastruktur und der Schulungsräume — Umsetzung CIP

V01.00, 28.06.2007 09:59:	neu (We)
V01.01, 23.07.2007 12:16:	Installation Esprimo als Büro-PC (We).
V01.02, 31.07.2007 11:43:	(immer noch) Esprimo-W2K-Treiber-Problematik.
V01.03, 03.08.2007 09:05:	Konsequenzen der IP-Umstellung; Netz-Altlastsanierung.
V01.04, 13.08.2007 09:05:	Backup, Restore, Clone (Workstations).
V01.05, 27.08.2007 09:21:	SW-Umzug GWT (We); Sophos-Install. (Seidel).
V01.06, 01.09.2007 10:50:	File-Server-Details, Anf. Primergy-Installation (We)
V01.07, 12.09.2007 10:28:	Sophos-Klarstellungen, &, div. Kleinigkeiten
V01.08, 27.09.2007 09:33:	LabView Anm., Résumée, Klone-Anleitung aktualisiert.
V01.09, 16.11.2007 11:58:	Abspaltung Hardwareteil (in [12]).
V01.10, 19.11.2007 12:14:	Kleinere Ergänzungen.
V01.11, 03.12.2007 12:16:	Ergänzung zum Print-Server.
Version: V1.11	

Zuletzt geändert von A. Weinert am 09.01.2008

Inhalt

1. Zweck, Umfeld, Voraussetzungen

Im Jahr 2005 stellte das Labor für Medien und verteilte Anwendungen der Hochschule Bochum einen Erneuerungsantrag für den vom Labor betriebenen sogenannten CIP-Pool. Im Juni 2007 wurde dieser (in Person von Seidel und Weinert gestellte) CIP-Antrag zugeteilt. Der Antrag betrifft die studentischen Schulungsräume und Labore sowie als zugehörige IT-Infrastruktur die Domain FB3-MEVA (Win2K, AD). Ein Ziel ist die Erneuerung der teilweise über 7 Jahre alten und mittlerweile unzuverlässigen Hardware (Bild 1). Daüber hinaus stehen wesentliche Modernisierungen und Verbesserungen der Software und der IT-Struktur (einschließlich endlich der Reparatur alter Fehler) an.
Die Ziele:

- zeitgemäße studentische Laborarbeitsplätze für die nächsten 5 Jahre (Bild1)
- Server-, Domain-, IT-Infrastruktur für die Schulungsräume und Labore (Bild 2)
- Verbesserte IT-Infrastruktur mit FH-weiten Angeboten und Diensten (file, print, application) für die ca. 4000 (Stand Anfang 2007) Nutzer (-konten) der Domain FB3-MEVA

Nach geltenden Bedingungen muss der zugeteilte Antrag rasch — das heißt innerhalb von drei Monaten bzw. zumindest im selben Jahr — umgesetzt werden. Angesichts des Vorlesungs- und Laborbetriebs kamen also nur die Monate Juli und August 2007 in Frage.

Bild 1: Der große Schulungsraum (Ausgangslage mit 7 Jahre alten Geräten)

Die Terminsituation wurde durch weitere zu koordinierende Baumaßnahmen, wie u.a. die Klimatisierung / Kühlung des zweiten Server- / Netzwerkraums komplizierter.

Durch die Änderungen mit dem "Hochschulfreiheitsgesetz" war dies übrigens der letzte zugeteilte CIP-Antrag der Fachhochschule Bochum, wenn nicht gar landeweit.

Das Vorliegende und [12] spezifizieren und dokumentieren die zugehörigen Arbeiten nachvollziehbar. Es kann und soll auch Anleitung und Tipps für spätere ähnliche Arbeiten dienen. Der Ausgangszustand der Domain FB3-MEVA wurde 2005 durch eine Migration von NT4 nach Server 2003 erstellt. Dieser Schritt ist in [9] ausführlich beschrieben. Die verwendete jüngste Hardware war damals schon fünf Jahre alt.

Was sich direkt hierauf bezieht oder demgegenüber nichts ändert ist im Vorliegenden ganz knapp gehalten oder weggelassen worden (siehe dann jeweils [9]). Einiges aber hat sich geändert, war gegenüber dem Ausgangszustand zu verbessern und wurde durch inzwischen erfolgte Änderungen Microsofts deutlich komplizierter.

Wie bereits angedeutet wurde diese Dokumentation (wegen des Umfangs) ab Version 1.09 in zwei Teile getrennt:

- eine Hardwareteil [12], der sich mit der Installation und Inbetriebnahme der Server und Workstations befasst
- und eine Software- und Betriebssystemteil <10> (das Vorliegende),, der die Umstellungen und Modernisierungen der Domäne, des Active Directory und der IT-Infrastruktur zum Gegenstand hat.

2. Server - Grundinstallation

In diesem Kapitel werden Anforderungen (im Lastenheftsinne) an die Server gesammelt. Dies geschieht nur stichwortartig und nur, soweit sie von der vorangehenden Konfiguration (von 2002, vgl. [9]) abweichen.

In diesem Lastenheftsinne beschreibt dieses Kapitel auch keine Arbeitsabläufe; diese finden sich in späteren Kapiteln bzw. in [12] und können auch für andere Verhältnisse als Tipp dienen.

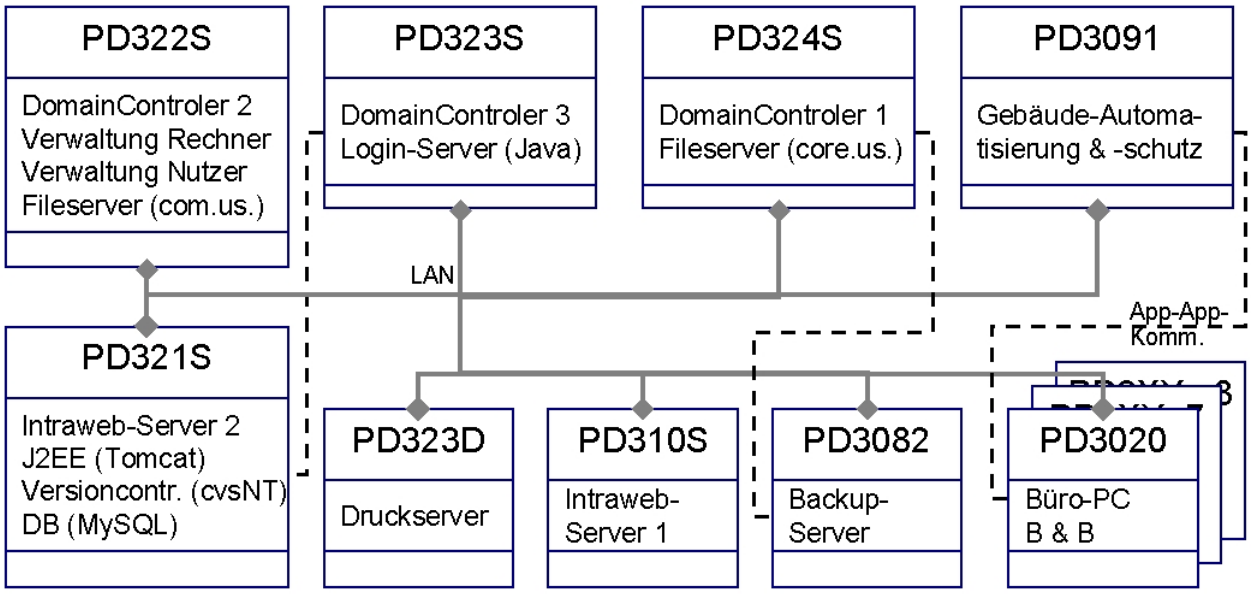

Bild 2: Domain-Controller und einige Application-Server (Ausgangslage).

2.1 Basisbetriebssystem für Server

Betriebssystem für alle Server ist

- Windows Server 2003 enterprise edition

im der jeweils aktuellen Updatezustand (August 2007 : Servicepack 2).

2.2 Domain Controller

Die bisherigen drei Domaincontroller sollen um einen vierten ergänzt werden. Dieser vierte soll über eine Routerfunktion auch Rechner als Domainmitglieder in einem privaten Netz bedienen.

Die DCs sollen von ihren bisherigen Zusatzfunktionen (file, application) im Sinne einer klaren Funktionstrennung entlastet werden. Diese Funktionen werden auf dedizierte Server ausgelagert.

Aus Gründen der Einfachheit und Beherrschbarkeit werden dies zunächst reale Server sein. Aus Kosten und Auslastungsgründen sind hierzu später auch virtuelle Server angedacht. (Fileserver werden / bleiben dedizierte reale Maschinen.)

Alle DCs sind auch DNS-Server. Der vierte oben erwähnte DC macht (nur, s.u.) für sein privates Netz auch DHCP.

Regeln für die Netzwerkkonfiguration von DCs

- Die IP-Adresse wird vom FH-DHCP bezogen;
  Ja [sic!], auch wenn es auf den ersten Blick unsinnig erscheint *1)
- Die DNS-Suffixsuchliste bekommt folgende Einträge in dieser Reihenfolge
  1. FB3-MEVA.fh-bochum.de
  2. fh-bochum.de
- Der erste DNS-Eintrag ist der DC selbst (oder der PDC GCS).
- Der zweite DNS-Eintrag ist anderer DC
- Der dritte Eintrag ist ein FH-DNS:
  193.175.112.3 (pav030.fh-bochum.de) und/oder 195.37.168.3

Für die übrigen Server gelten die selben Netzwerk-Konfigurationsregeln wie für die Workstations der Domain (s.u.).

Anmerkung *1): Das DNS und DHCP der FH (also das der Firma) muss eh alle Domain-Server und Workstations richtig und konsistent mit dem DNS / AD der Domain führen. Läuft dies auseinander (z.B. wegen unangekündigter Änderungen durch die FH-DVZ) bekommt man so oder so massive Probleme. Der feste Eintrag der richtigen IP (aus Domain-Sicht) hilft dann auch nichts mehr. Also kann man das FH-DHCP wenigsten für diesen Teil (IP-Vergabe) nutzen,

2.3 File - Server

Hintergrund

Die Domain FB3-MEVA bietet seit Jahren einen hochschulweiten file-service für alle ihre mehr als 3000 persönlichen (überwiegend studentischen) Nutzer. Die Nutzer können ihre Daten von jeder Workstation, die im FH-Netz Zugriff zur Domain FB3-MEVA hat, nutzen. Das geht einfach mit

```
net use Z: \\193.175.115.15\<freigabe>[\<user>]  *
                    /user:FB3-meva\<user> /persistent:no
```

(Server-Namen bzw. -IP-Adressen siehe unten oder unter . http://www.a-weinert.de/service/fileservice.html.)

Daneben gibt es keinen hochschulweiten file service.

Ausgangslage

Die Domain-Controller wurden als File-Server mitbenutzt (vgl. Bild 2 oben). Dagegen spricht prinzipiell nichts, nur sind inzwischen Grenzen bei Kapazität, Leistung und Administrierbarkeit erreicht.

Obgleich ein Back-up als Eigenschaft nicht versprochen wird, gab es einen gemeinsamen (betagten) Backup-Server für die o.g. div. File-Server. Für diesen sind die genannten Grenzen inzwischen weit überschritten.

Bis August 2007 wurde der DC

- PD324S (193.175.115.2)

als File-Server für Kern- (Team-) Aufgaben der Domain FB3-MEVA genutzt und der DC

- PD322S (193.175.115.4)

als File-Server für Alle und insbesondere für die vielen Studierenden-Konten.

Die Verbindung zum fileserver, sprich die Zuordnung eines Laufwerks (Z:), erreicht man mit einem Befehl net use; siehe oben.

File - Server - Struktur ab September 2007

Zwei gleiche File-Server mit hinreichender Kapazität und RAID (1 / 5) kommen in unterschiedliche Server-Räume. Ihr Inhalt wird einmal nächtlich gegenseitig aktualisiert.

Zur Lastverteilung dienen sie jeweils den oben genannten unterschiedlichen Nutzerbereichen "Kernaufgaben" und "Alle" als primärer File-Server.

	Domain-DNS	bis August 2007		ab September 2007	
Bereich	**Alias**	**Name**	**IP**	**Name**	**IP**
Kernteam	coreFileServer	PD324S	193.175.115.2	PD327S	193.175.115.14
Alle	studFileServer	PD324S	193.175.115.4	PD337S	193.175.115.15

Die Aliase im Domain-DNS können bei Änderungen Ausfällen oder Wartungsarbeiten geändert oder auch tageweise auf die redundante Maschine umgeschaltet werden.

Die schon aus diesem Grunde vorzuziehende direkte Verwendung von Aliasen für Rollennamen anstatt der Rechnernamen oder gar der IP scheitert allerdings daran, dass Freigaben mit Aliasen nicht funktionieren (ja teilweise nicht mal mit Rechnernamen).

Eine händische oder programmierte Auflösung des Alias und
dann Verwendung der IP ist aber immer machbar:

```
...>  nslookup studFileServer pd323s
DNS-Server: pd323s.fb3-meva.fh-bochum.de Address: 193.175.115.3
Name:       pd327s.FB3-MEVA.fh-bochum.de Address: 193.175.115.15
Aliases:  studFileServer.FB3-MEVA.fh-bochum.de
```

Hinweis: Im beispielhaftem nslookup-Befehl zur Auflösung des Aliases studFileServer muss als zweiter Parameter ein DNS-Server der Domain FB3-MEVA angegeben werden, wenn der betreffende Rechner nicht schon so eingerichtet ist.

Entsprechend der oben dargestellten Lastverteilungsrolle dient der jeweils andere File-Server als Backup. Dabei werden die Dateien des Kernteams einfach kopiert, womit gelöschte nicht verloren gehen. Umgekehrt sammelt sich jeder Mist "aufräumpflichtig" an, was im Kernteambereich ein geringes Problem ist. Beim übrigen Nutzerbereich ist das Backup ein Spiegel, bei dem spätestens nach 24 Stunden gelöschte Dateien auch weg sind.

Das Update-Script findet sich im Anhang.

2.4 Print - Server

Die Domain FB3-MEVA betreibt einen Druckdienst mit dem Printserver PD313D. Dieser Dienst umfasst neben einigen Domain-internen Druckern auch die hochschulweit aufgestellten Kopierer des internen Medienservice (IMS = Druckerei), soweit diese als Drucker nutzbar sind (siehe auch www.a-weinert.de/service/druckdienst.html).

Hinweis: Der Print-Service für einige der in der Hochschule aufgestellten Kopierer = Drucker (IMS C-Gebäude, Wirtschaft A-Gebäude) wird möglicherweise an die Verwaltungs-DV (F. Schulz) abgegeben werden. Der Print-Service für die im Bereich des MEVA-Lab (und der Fachbereichs Informatik) aufgestellten öffentlichen Bezahl-Drucker (Kopierer) bleibt (ggf. zusätzlich) in der Domain FB3-MEVA.

Alle für den Print-Service vorgesehenen Drucker werden im Printserver mit aktuellen Windows-Treibern installiert. Dies ist die Mindestausstattung an Treibern. Wenn der Druckerhersteller Treiber für weitere Betriebssysteme und Varianten liefert, können diese im Print-Server hinterlegt werden.
Hinweis: Für die NRG-Kopierer gibt es nur Windows-Treiber.

Alle Drucker im Druckserver werden freigegeben.

Für die Installation von solchen Druckern an Nicht-Domain-Rechnern durch die dortigen (Nicht-FB3-MEVA-) Administratoren gibt es einen speziellen Benutzer fb3-meva\vvv mit Passwort vvv, der ausschließlich dem installierenden Zugriff zum Print-Service dient.

Alle Drucker im Druckserver werden vorher mit den beabsichtigten Rechten versehen. Ein Bezahldrucker (=Kopierer mit Münzaotomat oder Kartenleser) bekommt natürlich Druckrecht für "Jeden". Jemanden dar dafür seitenweise bezahlt vom Drucken abzuhalten ist i.A. sinnlos.

Bild 3 zeigt diese Verhätnisse im Printserver.

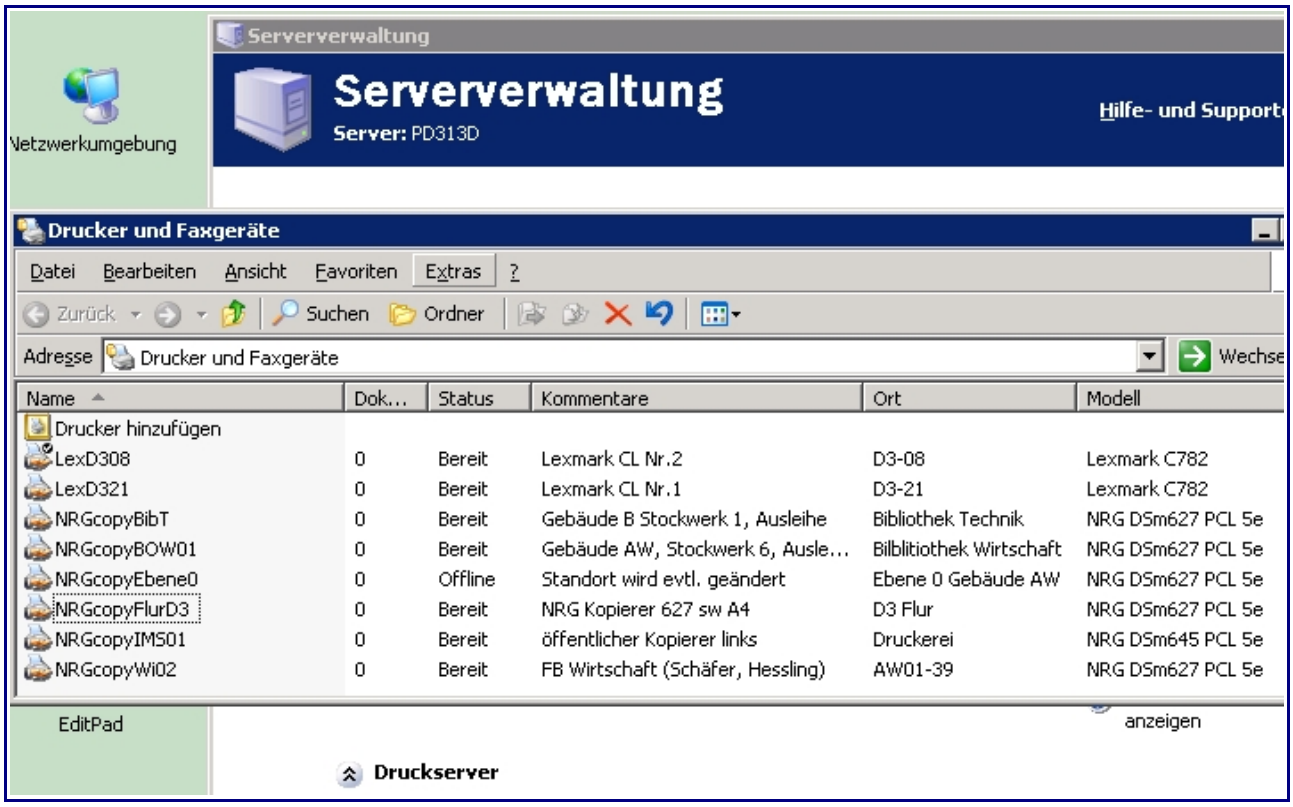

Bild 3: Die Drucker im Printserver (PD313D; alle freigegeben)

Bei einem Nicht-Domain-Rechner installiert sich der dortige Administrator soviele dieser Drucker von diesem Druckserver, wie er für sich und seine Anwender für sinnvoll hält. (Gegebenenfalls nutzt er dazu fb3-meva\vvv mit Passwort vvv, wie oben angedeutet.)

Für eine Rechner, der zur Domain gehört — einschließlich der Server und DCs — gilt sinngemäß das selbe. Lediglich bei Rechnern, bei denen eine administratover remote-Zugriff von einer Workstation (eines Administrators) zulässig sind — und dies sind i.A. alle Server und DCs —, sollte die Auswahl der vom Druckserver dort zu installierenden Drucker etwas ausgeweitet werde. Es sollten alle Drucker installiert sein, die man auf der remote-Workstation (der mit der Terminal-Rolle) auch vorfindet. Zuwiderhandlung ist an sich unschädlich, führt aber meist zu langen "Ich konnte Treiber nicht finden"-Beschwerden in System-Logs, die deren Auswertung nicht gerade erleichtern.

Bild 4 zeigt diese Verhältnisse für einen Rechner der Domain. (Im Beispiel ist es der Domain-Controller PD313S, aber das ist hier unwesentlich.).

Ein Umstand ist hier noch wichtig, da ggf. fehlerträchtig. Bei einem Blick auf vom Druckserver kommende Drucker — direkt oder remote à la Bild 4 — sieht man die Drucker freigegeben. Dies ist keine lokale Freigabe dieser Drucker auf dem betreffenden Rechner sondern indirekt die (selbstverständliche) Freigabe des betreffenden Druckers auf dem Druckserver.

Hinweis, Falle: Beseitigt man mit entsprechenden Rechten diese Freigabe auf dem lokalen Rechner ist die Freigabe auf dem Druckserver weg — und damit dieser Drucker für die meisten seiner Nutzer. In der graphischen Anzeige sieht man den Unterschied zwischen einer "richtigen" und einer "indirekten" Freigabe noch am "kleinen Händchen" (Bild 4) statt "großen Händchen" (Bild 3). Bei der Kommandozeile oder dem Eigenschaftsfenster ist dieser Unterschied aber weg.

Bild 4: Einige Drucker des Printservers in einem Domain-Rechner

2.5 Web Server und administrative Web-Dienste

Grundlage hierfür sind J2EE mit dem Container Tomcat.

Ziel ist das Darstellen (B&B) aller administrativen und sonstigen als Webservices; ein Mittel dazu kann AJAX mit GWT sein.

2.5 Sonstige Application Server

Hierunter fallen unter Anderem

- Objektschutzsystem
- Versionsverwaltungen (cvsNT, ~~Subversion~~)
- Datenbanken (mySQL, ~~cachè~~)

Anmerkung: Soweit sich gegenüber der vorherigen Installation Änderungen ergeben, werden diese später beschrieben.

2.6 License Server

Anmerkung zu Lizenzservern

Der oberste Grundsatz muss sein: **Vermeiden!**

Software mit der Notwendigkeit von Lizenzservern ist in der Lehre in einem Umfeld mit Tausenden von studentischen Nutzerkonten / Nutzern, die Dutzende von Workstations frei wählbar nutzen erfahrungsgemäß nicht störungsfrei zu betreiben.

Übrigens: Erfahrungen (leider nur) anderer Hochschulen zeigen, dass bei vernünftigen, aber hartnäckigen Verhandlungen mit den Lieferanten industrieller Software, diese durchaus für den Lehrbetrieb — und teilweise sogar für die studentische Hausarbeit — geeignete Versionen "herausrücken", statt mit dem Standardverkaufsprodukt nur Ärger zu

bereiten. Schließlich ist es das ureigenste Interesse des jeweiligen Lieferanten, Studierende an "seine" CAD-, Automatisierungs-, Simulations- etc. Software zu gewöhnen.

Wegen der angedeuteten erheblichen administrativen Probleme mit den Lizenzservern wurden diese bisher häufig in dedizierten (leistungsarmen und für was Gescheites unverwendbaren) Rechnern in die Verbannung geschickt. Mit der (geplanten) Befreiung aller DCs von File-Server-Aufgaben sollte in Zukunft ein DC (PD322S), soweit möglich, alle Lizenzserver-Aufgaben übernehmen.

Im DC PD322S installierte Lizenzserver werden grundsätzlich nicht redundiert. Da in diesem DC auch die Dienste für das Anmelden an studentischen Laborarbeitsplätzen laufen, ist ggf. der gleichzeitige Ausfall der Lizenzen eher gewollt.

Diese Installation von Lizenzservern auf Domain-Controllern wurde bereits bitter bereut. Bei gewissen Unpässlichkeiten laussen die lmtools in einen Zustand, in dem sie mehrere Prozessorkerne zu 100% auslasten. Und diese denial of service attack auf einen DC bringt seinerseits den ganzen Rest ins Wanken.

3. Workstation — Grundinstallation

In diesem Kapitel werden Anforderungen (im Lastenheftsinne) an die Workstations gesammelt. Dies geschieht nur stichwortartig und nur, soweit sie von der bisherigen (fünf Jahre alten) Konfiguration abweichen. In diesem Sinne beschreibt dieses Kapitel auch keine Arbeitsabläufe; diese finden sich (ausgelagert) in [12].

3.1 Basisbetriebssystem

Betriebssystem für die überwiegende Zahl der Workstations ist

- Windows **Server 2003** enterprise edition

im der jeweils aktuellen Updatezustand (im August 2007: Servicepack 2).

Software mit besonderen Anforderungen an das Betriebssystem, seinen Updatezustand oder mit Unverträglichkeiten zu anderer Software bekommen bei den Standard-Workstations eine eigene Ablaufumgebung:

- andere Systeme und Updatezustände mit VMware (-player)

Zu solcher Software mit unverträglichen Anforderungen gehören u.A. Siemens WinCC und Siemens PCS7.

Für Laborrechner mit Sonderfunktionen und -hardware kommt ausnahmsweise

- Windows XP enterprise edition

im der jeweils aktuellen Updatezustand zum Einsatz.

In diese XP-Kategorie fallen Workstations mit Anschluss an dSpace-Hardware. dSpace kann angeblich nur mit XP und nicht mit einem Server-Betriebssystem arbeiten. Ebenso gehören hierher Siemens-Labtops (Lifebook E) wegen fehlender Treiberunterstützung für Server 2003.

Regeln für die Netzwerkkonfiguration von Workstations der Domain

- IP-Adresse wird vom FH-DHCP bezogen [sic! trotz Domain]

- Die DNS-Suffixsuchliste bekommt folgende Einträge in dieser Reihenfolge
    1. FB3-MEVA.fh-bochum.de
    2. fh-bochum.de
- 1. [2.] DNS ist ins ein Domain DNS (i.A. also ein DC).
- nur optional letzter [letzter -1] DNS ist ein FH-DNS (s.o.))

Es ist unabdingbar, dass der erste DNS-Eintrag eines Rechners der Domain ein Domain-DNS (=DC) ist. Das für die Zuteilung der IP-Adresse aus anderen Gründen verwendete FH-DHPC kann keine Service-Einträge entgegennehmen und es liefert auch leider nicht die FB3-MEVA-Einstellungen.

Ob man überhaupt ein FH-DNS (die ändern sich ab und zu unangekündigt) als Name-Server an letzter Position einträgt, hängt davon ab, ob der Rechner in dem konstruierten Falle, dass das FH-Netzwerk noch geht aber kein einziger DC erreichbar ist, verwendbar sein soll / kann.

Die IP-Konfiguration eines Domain-Mitglieds muss sinngemäß so aussehen:

```
Windows-IP-Konfiguration

   Hostname  . . . . . . . . . . . . : pd3022
   Primäres DNS-Suffix . . . . . . . : FB3-MEVA.fh-bochum.de
   DNS-Suffixsuchliste . . . . . . . : FB3-MEVA.fh-bochum.de
                                       fh-bochum.de

Ethernet-Adapter LAN-Verbindung:

   Verbindungsspezifisches DNS-Suffix: fh-bochum.de
   Physikalische Adresse . . . . . . : 00-19-99-03-16-0F
   DHCP aktiviert  . . . . . . . . . : Ja
   Autokonfiguration aktiviert . . . : Ja
   IP-Adresse. . . . . . . . . . . . : 193.175.115.28
   Subnetzmaske  . . . . . . . . . . : 255.255.255.0
   Standardgateway . . . . . . . . . : 193.175.115.1
   DHCP-Server . . . . . . . . . . . : 193.175.112.15       // FH-DHCP
   DNS-Server  . . . . . . . . . . . : 193.175.115.2       // DC
                                       199.175.115.3      // DC
                                       193.175.112.3     // FH-DNS
   Primärer WINS-Server  . . . . . . : 193.175.112.110  // FH-WINS
   Lease erhalten / Lease läuft ab . : Montag, ....
```

3.2 Administrative Basissoftware

Java JDK / JRE 1.6

Login-LDAP Software (Java; LogAlert / LogServer)

remote Login (für die Domain-Administratoren)

Windows – update (WSUS); automatisch Laden, aber Installieren. nur mit Zustimmung eines Administrators.

Logoff-Screen-Saver

3.2 Arbeitssoftware

Java JDK / JRE 1.6_2

Eclipse 3.3 ("Europa")

Borland C 5.5, [sic] genau das wegen DLLs und µCs

Editpad

~~FireFox~~ (ersetzt durch Seamonkey, da Firefox angeblich hinfort nicht mehr gepflegt wird)

Seamonkey (Nachfolger von Mozilla / Firefox)
Dies war eine Fehlinterpretation. Es wird aus Firefox "zurückgeschaltet".

Thunderbird (?; zunächst nicht; siehe unten Anmerkung zu mail-client)

FASM (flat assembler)

Staroffice 8 (jeweils mit aktuellstem Update)

MS-Office (2000 premium)

GWT (Google Web Toolkit)

SciLab (kann MatLab, s.u., ersetzen)

Anmerkung zu einem e-Mail-Client: Es müsste ggf. ein mail-client gefunden werden, der ohne zusätzlichen Eingriff, den e-mail-account eines "zweistufig" (vgl. Benutzerverwaltung) angemeldeten Studierenden bietet. Dies könnte z.B. dadurch geschehen, dass er ohne jedes wenn und aber alle account-Einstellungen von einem Netzlaufwerk (dem file-Server-Bereich des Angemeldeten) bezieht. Die Mozilla-Konsorten "denken" hierbei viel zu komplex, auch in teilweise registry- bzw. "Dokumente und Einstellungen-"basierten Profilen.

3.3 Sondersoftware

In dies Kategorie fällt diejenige Software für Schulungs- und Laborrechner, die im Vergleich zu ihrem Nutzen einen unverhältnismäßig hohen, ja teilweise unvertretbaren, Administrierungsaufwand erfordert. Dies ist meist zwei Ursachen geschuldet:

- Notwendigkeit eines Lizenzservers und / oder Rechner- oder Nutzer-individuellen Lizenzeinstellungen.
  Dies ist mit über 60 gleichen Schulungsrechnern und Tausenden von studentischen Nutzerkonten kaum vereinbar.
  Beispiele für solche Software sind u.A. AutoCad und EPlan.
- Unverträglichkeit der Software mit anderer Standardsoftware und / oder Betriebssystemaktualisierungen.
  Beispiele hierfür sind WinCC und PCS7, die sich nicht mal untereinander in der selben Plattform vertragen, sowie auch dSpace.

Liste der Sondersoftware

MathWorks Matlab (R2007a)

Autodesk AutoCAD 2008

LabView

Hinweis / Warnung zu LabView: Labview auf einer Workstation mit allen legalen Lizenzen etc. richtig installiert erwies sich einfach als "root kit". Die vorher übersichtliche und funktionierende Liste der Geräte (Computerverwaltung) wird fünf mal solang; und diese sind vielfach unbehebbar gestört. Ähnliches gilt für Dienste und vorher nie auftretende Systemmeldungen (nun ellenlange logs). Der Rechner wird bis um den Faktor 8 langsamer, auch ohne dass LabView benutzt wird. Deaktivieren der gestörten geheimnisvollen Geräte (um den Unzustand des unzumutbar langsamen Systems mit Log-Meldeschwällen zu beheben) führt schließlich zum Verlust der Bootfähigkeit selbst im abgesicherten Modus [sic!).
Also Neu-Installation des kompletten Systems — und nie nie mehr LabView auf einem Rechner, der noch zu irgendwas Anderem taugen soll!

Siehe hierzu auch die entsprechenden Kapitel in [12].

4. Benutzerverwaltung

Benutzer und Seminarkonten

Benutzerkonten sind normale AD- / Domainkonten. An ihnen, als "security principal", hängen alle Rechte des Nutzers insbesondere seinen individuellen Dateirechte auf den File-Servern.

Alle FH-Angehörige können ein mit mit ihrem FH-LDAP-Namen gleichlautendes FB3-MEVA-Domain-Konto erhalten. Das FH-Namensschema ist

- SFB<fachbereichsnummer><indivNummer>
- MFB<fachbereichsnummer><indivNummer>
- DFB<fachbereichsnummer><indivNummer>
- AFB<fachbereichsnummer><indivNummer>

Dabei steht S für Studierende, M für Mitarbeiter, D für Dozenten und A für Sonderkonten; ein Beispiel für ein Studierendenkonto des Fachbereichs Informatik (FB3) ist

- SFB30700

Bestimmte Dienste, auch Webdienste, synchronisieren das Passwort der "SFB-/DFB-/MFB-" Konten der Domain FB3-MEVA mit dem LDAP der FH.

Ein Seminarkonto ist aus Domain- / AD-Sicht ein normales Nutzerkonto. Es dient aber vielen studentischen Nutzern zur gleichzeitigen Anmeldung an bestimmten Rechnern und hat dafür ein quasi öffentliches Passwort.

Die eigentliche Authentifizierung erfolgt in einer zweiten Stufe mit dem jeweiligen AD- / Domain- / LDAP- Konto des Nutzers und seinem (geheimen) Passwort.

Zweistufige Anmeldung

Die bewährte "zweistufige Anmeldung" (siehe [9] und Bild) wird im Wesentlichen unverändert beibehalten. Die Anmeldung eines studentischen Einzelnutzerkontos an einer Labor-Workstation erfolgt in folgenden Schritten:

- Windowsanmeldung mit einem der (wenigen) Seminarkonten (studi, studiXP etc.)
- In einem zweiten Anmeldefenster (Bild) Abfrage eines dem LDAP- / FH-Email-Konto entsprechenden Einzelkontos (sfb3i007 z.B.) und Passworts.
  Das zweite Fenster und die Kommunikation mit den Servern etc., sprich das meiste Folgende, macht die Anwendung LogAlert.
  (LogAlert.java in LogAlert.jar benötigt a_weinertBib.jar)
- Authentifizieren des Namen-/Passwort-Paares beim zentralen LDAP-Server (der FH).

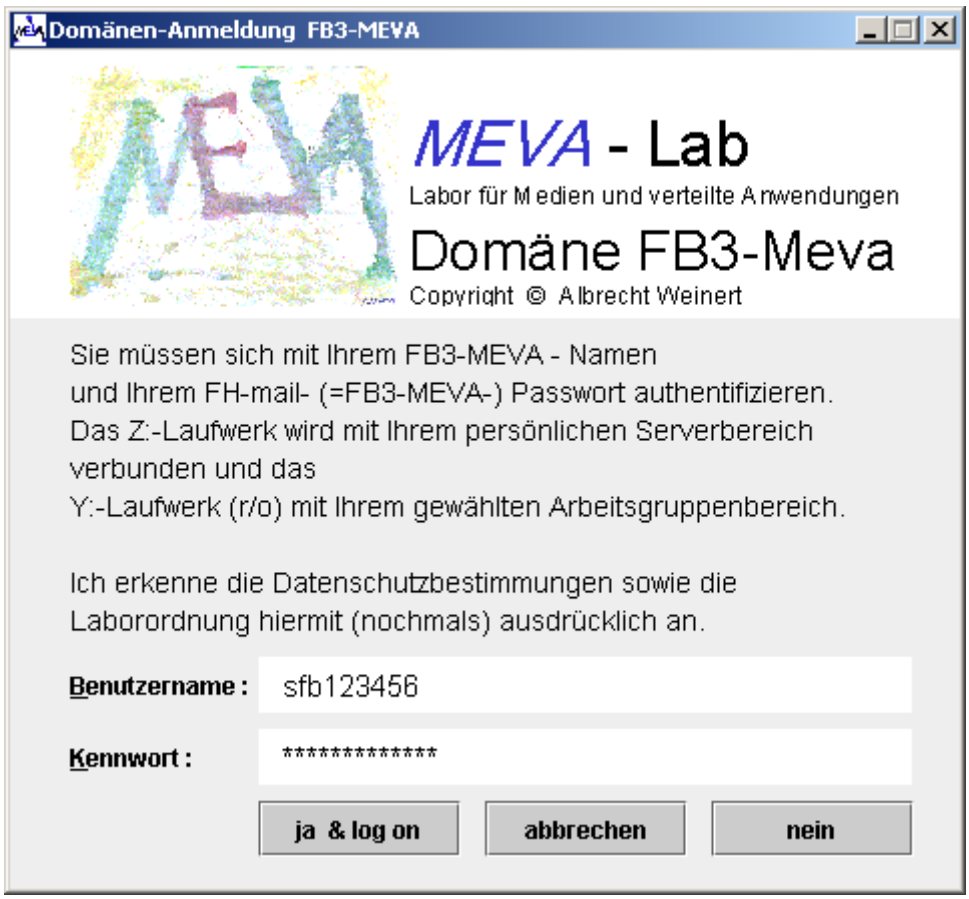

Bild 5: Zweites Anmeldefenster der "zweistufigen Anmeldung" (LogAlert.java)

- Ein Misslingen dieser LDAP-Authentifizierung bedeutet keine direkte Ablehnung; dies geschieht aber ggf. indirekt in den folgenden Schritten.
  Diese Barmherzigkeit duldet zum einen „ungeLDAPte“ Konten, die man gelegentlich benötigt (Muster-Student); zum zweiten toleriert sie gelegentliche Ausfälle des zentralen LDAP oder der Verbindung dorthin.
- Ausfälle des zentralen LDAP 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 DC.
- Authentifiziert durch Einzelkonto (sfb3i007 z.B.) Verbindung mit dem Gruppen-Fileserver-Bereich (Y:-Laufwerk, \\freigabe\studi\ zum Beispiel).
  Für diesen Bereich haben eine oder mehrere der Gruppen CAX, SPS etc. Lese- und Ausführungsrecht.
  Dieser Schritt misslingt, wenn das Einzelkonto (sfb3i007 z.B.) nicht Mitglied einer der betreffenden Gruppen ist.
  Diese Gruppenmitgliedschaft ist somit genau das Privileg, sich via studi (im Beispiel) anzumelden.
- Authentifiziert durch Einzelkonto (sfb3i007 z.B.) Verbindung mit dem Gruppen-Fileserver-Bereich (Z:-Laufwerk, \\freigabe\(sfb3i007 im Beispiel).
  Für diesen Bereich hat der Benutzer (FB3-MEVA\sfb3i007 im Beispiel) Vollzugriff; es ist sein bzw. ihr persönlicher FH-weiter Fileserverbereich.
  Dieser Schritt misslingt, wenn das Einzelkonto nicht korrekt angelegt oder teilweise gelöscht oder gesperrt wurde.
- Suchen des Namens der Anmelde-Workstation (Computer-Name; PD3W727 z.B.) in einer Liste (r/o) im Gruppen-Fileserver-Bereich (Y:-Laufwerk).
  Diese Liste führt diejenigen Rechner auf, an denen sich das Seminarkonto (studi im Beispiel) anmelden darf.
  Dieser Schritt misslingt, wenn die verwendete Workstation nicht aufgeführt ist.

Ein Misserfolg in irgendeinem der Schritte (Ausnahme LDAP) beendet den Anmeldevorgang durch sofortige Zwangsabmeldung. Durch entsprechende Einstellungen, Anmeldeskripts und Tools wird ein „zwischendurch Herausmogeln“ und Arbeiten mit nur der (quasi öffentlich zugänglichen) Seminarkonten-Authentifizierung verhindert. Entscheidend dabei ist das so genannte „synchrone“ Laufen des Anmeldeskripts (vgl. auch Anhang) 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
               REG_SZ   CachedLogonsCount = 0
```

Dieser Registry-Einträge sind auf allen (!) erlaubten Workstations zu setzen.

Im Profil aller Gruppennutzer ist der “log off screensaver” (10 Minuten Inaktivität, 90 s Warnzeit) eingerichtet. Eine einschlafende Sitzung wird also innerhalb kurzer Warnzeit zwangsweise abgemeldet. Dies kann einem unaufmerksamen Nutzer zwar schaden. Dennoch ist diese Einstellung ist zum Schutz der individuellen (Einzel-) Nutzerdaten und seines persönlichen File-Server-Bereichs (des sfb3i007 im obigen Beispiel) notwendig, da selbst ein passwortbewehrter Bildschirmschoner hier nur das quasi öffentliche Seminarkonten-Passwort (von studi im Beispiel) verlangt.

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 Installations- oder Wartungs-Skripten (siehe Anhang).

Erzeugen eines Seminarkontos

Ein Seminarkonto im eingangs des Kapitels beschriebenen Sinne dient vielen (studentischen) Nutzern zur gleichzeitigen Anmeldung an bestimmten Rechnern und hat dafür ein quasi öffentliches Passwort. Die individuelle Authentifizierung erfolgt ggf., wie beschrieben, in einer zweiten Stufe.

Ein solches Seminarkonto hat grundsätzlich ein unveränderliches serverbasiertes Profil und einen ebenso unveränderlichen Fileserverbereich (R/O; Y:-Laufwerk bei zweistufiger Anmeldung).

Um ein neues Seminarkonto <zielname> (im Beispiel) nach dem Muster eines vorhandenen, <quellname> ("studi" im Beipiel) zu erzeugen, muss ein Administrator folgendes tun:

1. Auf einem Domaincontroller (PD322s) AD Konto <quellname> (in CN=mevaStGrp) nach <zielname> kopieren und anpassen.
2. Anmelden als <quellname> für ggf. letzte Änderungen am Profil; Abmelden.
3. Anmelden an der selben Workstation als Admin; mit Systemsteuerung Profil nach \\<server>\fb3stuPrf\<zielname> kopieren. Dabei Benutzer nach <zielname> ändern; siehe Bild 3.
4. Auf \\<server>\fb3stuPrf\<zielname> das gerade kopierte Profil änderbar machen (ntuser.dat); später Sperren (ntuser.man) nicht vergessen.
5. Auf dem Fileserver die (r/o) Daten für den neuen Seminarnutzer <zielname> erzeugen mit
   ...>roboComplete G:\fb3studf\ymuster\ G:\fb3stuPrf\<zielname>\
   und anschließend anpassen.
6. Als "<zielnutzer>" anmelden und Profil anpassen. (Nach Arbeit Sperren.)

Hinweis: Schritt 3. geht auch wenn Nutzer und Profil bereits vorhanden sind, um ein Profil mit den Einstellungen eines anderen zu überschreiben.
Das kopierte Profiel wird als ntuser.dat angelegt selbst wenn es bei der Quelle als nzuser.man gespert war.

Umbenennen eines Seminarkontos

Ein Seminarkonto umbenennen geht so:

1. Konto im AD umbenennen (dabei Anzeigename, Anmeldename und Feinheiten richtig setzen). Insbesondere Profilpfad umändern, (falls nicht mit %username% automatisiert).
2. Profilpfad umbenennen (so geht das, da die User-SID ja bleibt).
3. Y:-Laufwerksbereich umbenennen.

Nach diesen einfachen Schritten Anmelden an Workstation versuchen.

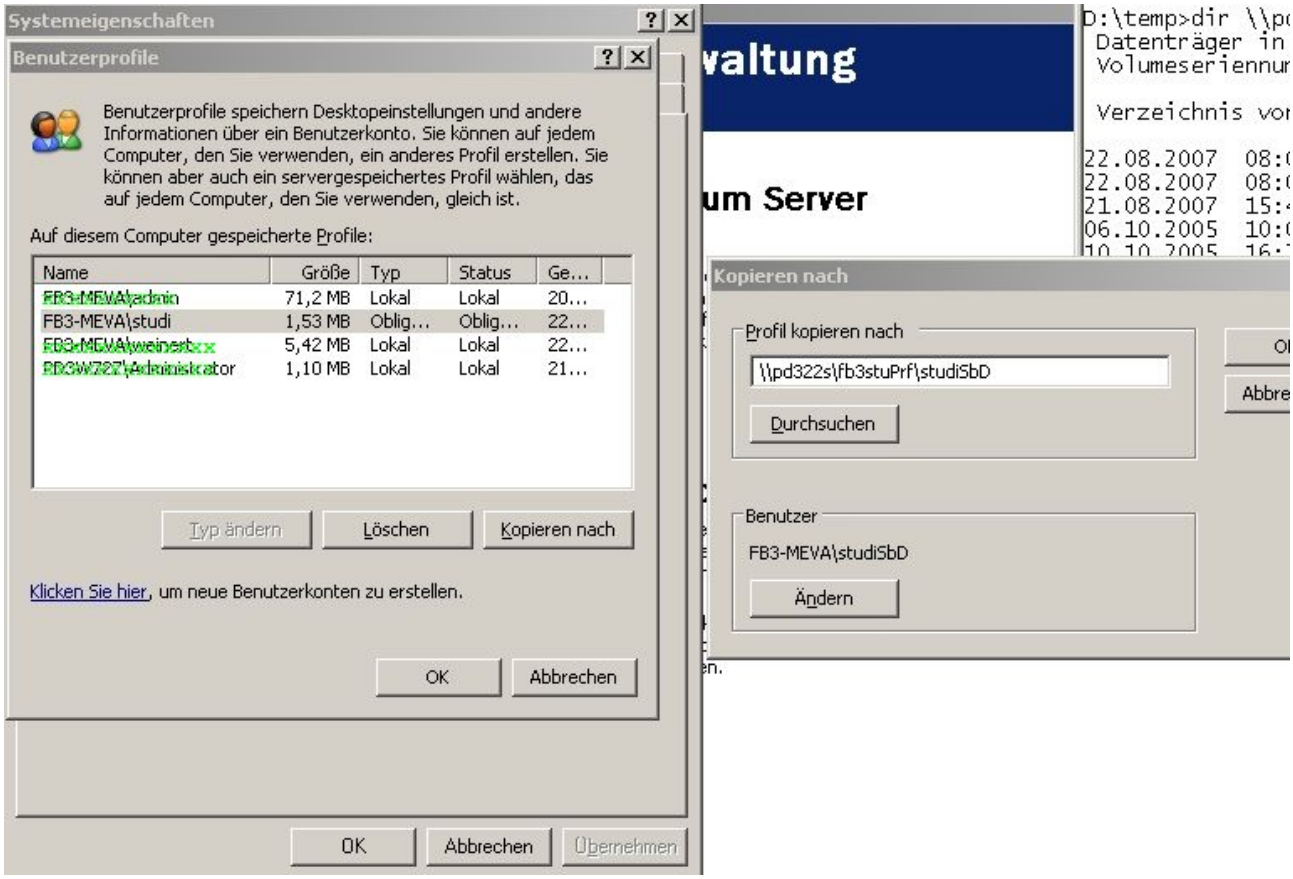

Bild 6: Kopieren eines Profils auf der davon zuletzt genutzten Workstation (als Admin)

Erzeugen eines persönlichen Kontos

Ein persönliches Konto sfb..., xfb... etc. kann mit einem Script auf einem Domaincontroller erstellt werden, dem die Informationen Kontenname (Hochschul-LDAP), Nachname, Vorname, Fachbereich, Studienrichtung und Semester bzw. bei Dozenten / Mitarbeitern Fachrichtung und Titel/Funktion geliefert werden. Diese Script erzeugt das Domain-Konto, macht alle AD-Einstellungen und erzeugt einen für studentisches Arbeiten vorkonfigurierten file-server-Bereich mit passenden Zugriffsrechten.

Für vom Studierendenservice gemeldete Erstsemester des Fachbereichs Informatik lässt ein Administrator diesen Vorgang vor Beginn eines Wintersemesters in einer Schleife laufen. Dies wird so seit Jahren mit etwa 90% Erfassungsquote gemacht.

Seit Oktober 2007 können alle Hochschulangehörige hochschulintern diesen Vorgang mit einem Web-Dienst auslösen, wenn sie sich gegen das Hochschul-LDAP authentifizieren können. Den Einstieg hierzu findet man (hochschulintern) unter

```
http://PD321S/
```

Die Domain FB3-MEVA steht mit all ihren Diensten so allen Hochschulangehörigen offen. Und die händische, administrative Nacharbeit für nicht erfasste Erstsemester, Gasthörer, Lehrbeauftragte, Hochschulwechsler etc. entfällt.

5. C-Netzmigration — Altlastsanierung

5.1 Hintergrund

Die FH Bochum verwendet in ihrem von der DVZ (FH-Rechenzentrum) internen (F&L-) LAN öffentliche C-Netzadressen, welche aber nicht nach außen sichtbar sind. Aufgrund diverser Organisationsmängel kam es dazu, dass der Domain FB3-MEVA Adressen in 10 unterschiedlichen C-Netzen zugeteilt wurden.

Die an sich unsinnige interne Verwendung öffentlicher Adresse ist geblieben, aber der Domain FB3-MEVA wurde ein zusammenhängender Block von IP-Adressen in einem C-Netz

- 193.175.115.xyz

zugewiesen.

Diese wünschenswerte Verbesserung (bzw. Behebung eines untragbaren Zustands) bedeutet für alle Rechner der Domain neue IP-Adressen bekommen. Dies betrifft auch alle

- Domain-Controller (DC),
- Nameserver (DNS) und
- andere Server (Lizenz, Print etc. pp)

und somit auch sämtliche fest eingetragene IP-Adressen in

- Netzwerkkonfigurationen,
- Konfigurationsdateien
- Scripten und Programmen.

5.2 Arbeitsschritte für DCs

Schritte für einen DC PD323S (erster im FH-DND+DHCP umgestellter DC):

- PD323S ist selbst runtergefahren (während der FH-Umstellung)
- Im DC PD324S für PD323S als 2. DNS die neue IP (193.175.115.003) eintragen
- In der DNS-Verwaltung des PD324S A-Eintrag für PD323S ändern
- und etwa 8 weitere verstreute Einträge
- In der DNS-Verwaltung des PD324S neue Reverse-Lookup-zone 193.175.115 anlegen. (Das wird irgendwann hoffentlich die einzige.

Schritte für zweiten DC PD322S:

- sinngemäß wie oben; ging (versehentlich) auch ohne runter Fahren
- Einträge in DNS ändern (es gab weniger verstreute).

Insgesamt wird die Umstellung der DCs=DNS mit jedem weiteren einfacher; die Umstellung des GCS/PDC als letzter lief fast automatisch.

5.3 Konsequenzen der IP-Umstellung

Die IP-Adressen von DCs, DNS, Applikationsservern ja sogar von Rechnern sind (leider) an zahlreichen Stellen hinterlegt. Alle diese Stellen müssen im Rahmen einer Umstellung, wie der hier geschilderten, gefunden und angefasst werden.

DNS-Einträge in jedem Rechner

Die Netzwerkeinstellungsregeln (s.o.) sehen bei jedem Domain-Rechner notwendigerweise vor, dass DC = DNS als erste Name-Server eingetragen werden. Da das FH-DHCP diesen Dienst nicht für die Domain FB3-MEVA leistet, müssen diese Eintrage fest eingestellt sein. Im Rahmen der "C-Netz-Sanierung" müssen bei allen bestehenden Mitgliedsrechnern, diese Einträge von Hand geändert werden.

Hinweis: Ein (wirklich) geeignetes Kommandozeilen-Tool für die Netzwerkeinstellung in einem Zug (möglichst remote) wurde noch nicht gefunden.

Tomcat - Konfigurationsdaten

In den folgenden Stellen der Konfigurationsdateien sind die jeweils geänderten IP-Adressen einzutragen.

server.xml (eine von mehreren, Auszug):

```
<Realm name="ADsso"
   className="org.apache.catalina.realm.JNDIRealm" debug="999"
      connectionURL="ldap://195.37.168.187:389"
      alternateURL="ldap://193.175.113.245:389"

      connectionName="CN=ldap reader,CN=Users,DC=FB3-MEVA,DC=fh-
bochum,DC=de">
```

Servlets – Java- (J2EE) - Quellen

In den entsprechenden Stellen der Quellen und Konfigurationsdateien (.xml, .properties) sind die jeweils geänderten IP-Adressen einzutragen.

KernTsk.java (Beispiel, Auszug):

```
/** LDAP-Server für (zusätzliche / Domain-) Authentifizierung. <br />
 *  <br />
 *  default: ldap://195.37.168.187:389<br />
 *  alternativ:  ldap://193.175.113.245:389<br />
 *  <br />
 *  @see LDAPauthRead#authByAD(String, String, String, String)
 */
    public String ldap2URL = "ldap://195.37.168.187:389";
```

Dies betraf auch die Java-Anwendung LogAlert.java für die "zweistufige Angeldung" (vgl. [9]) bzw. ihre Konfigurationsdatei (LogAlert.properties).

Anmelde-Scripte und zugehörige Anleitungsdateien (.bat, .cmd, .html, .pdf)

In den entsprechenden Stellen der Scripte (.bat, .cmd) und der Anleitungen (.html; .pdf, etc. sind die jeweils geänderten IP-Adressen einzutragen.

fileservice.html (Beispiel, Auszug):

```
In diesem Falle trennen Sie <strike>--</strike> entgegen Bill
Gates Anweisung <strike>--</strike> garnichts, sondern verwenden
(als &quot;work around&quot;) anstelle des Servernamens (PD322S)
dessen IP-Adresse mit sinngemäß dem folgenden Befehl:<br />
<br />    
       net use Z:  /user:FB3-MEVA\sfb3xyz
                  \\193.175.113.245\fb3stud\sfb3xyz
                    /PERSISTENT:NO          <br />
<br />
Wenn dies auch nicht geht, lesen Sie das nächste Kapitel.<br />
```

Hinweis: Auch druckdienst.html (ähnliche Stellen).

Und sonst?

Es wäre naiv anzunehmen, die aufgeführten Stellen wären schon alle. Bestimmt finden sich noch Stellen mit eingetragenen IP-Adressen von Rechnern. Kandidaten sind irgendwelche Listen in Lizenzservern (die eh immer für jeden Ärger gut sind).

Ebenso gern übersehene Stellen sind Einträge für LDAP-Server tief im AD-Baum. Wenn man die beim Durchforsten nach bisherigen (alten) IP-Adressen nicht erwischt, gehen LDAP-Anfragen ans AD nicht oder schlimmer, nicht zuverlässig.

5.4 Résumée der IP-Umstellung

Die Umstellung der DCs und DNS-Server lief (erstaunlich) einfach.

Lästig, arbeitsintensiv und fehlerträchtig ist das Finden und Nacharbeiten hunderter Stellen, in denen notwendigerweise oder aus Leistungsgründen IP-Adressen fest eingetragen sind.

Die Umstellung vieler IP-Adressen in einer Domain ist also durchaus machbar und gefährdet den produktiven Betrieb nur mäßig. Eine Umbenennung beispielsweise von

- FB3-MEVA.fh-bochum.de

nach

- FBI-MEVA.hochschule-bochum.de

oder Ähnliches liefe hingegen auf eine Zerstörung dieser IT-Infrastruktur hinaus.

6. Résumée

Die hard- und softwareseitige Renovierung und Modernisierung einer Windows-Server-2003-Domain mit hochschulweiten Diensten und Tausenden von Konten und etwa 100 Rechnern ist eine umfangreiche Aufgabe, die zwei bis drei qualifizierte Leute mehrere Monate beschäftigt.

Dabei waren und sind noch (Stand September 2007) schon die "straight forward" Installations- und Umbauarbeiten aufwändig genug. Dies ist aber normal und einigermaßen planbar. Wirklich störend und ärgerlich sind aber Rückschläge durch Unzulänglichkeiten der Produkte, ihrer Dokumentation und in manchen Fällen dem Support. Mit so etwas muss man natürlich rechnen und man kann es teilweise auch. Bei diesem Projekt waren solche Rückschläge in ihrer Zahl und gravierenden Auswirkung — gerade im Vergleich mit drei bzw. sechs Jahre vorher "gestemmten" ähnlichen Aufgabe (siehe [9]) — nun doch überraschend.

Zu den "Hits" zählen

- die root-Kit-Eigenschaften der LabView-Installation
- die Inkompatibilität der (zu einem gemeinsam erarbeiteten Angebot gehörenden) Siemens-Hardware
- Klone- und Backup-Tools die (dank Linux-Herkunft) nicht zuverlässig mit Windows-Laufwerken und -Partitionen umgehen können (Acronis) oder Server 2003 nicht bearbeiten wollen (Norton Ghost).

Würde Microsoft das im gegebenen Umfeld unabdingbare Klonen von Workstation- und auch Server-Installationen einfach unterstützen (statt es eher noch zu hindern), wäre Platz drei auf dieser Hitparade weg.

Als zwar arbeitsaufwändig aber überraschend unproblematisch — gerade hier lagen in der Projekt-Vorplanung eher die Bedenken, wenn nicht gar Ängste — hat sich die Umstellung der Domain auf komplett neue IP-Adressen erwiesen, mit der ein Mangel der bisherigen Einbindung in die Hochschul-IT beseitigt wurde. Dasselbe kann positiv über die Umstellung der Fileserver bzw. das "Aufbohren" des ja hochschulweit gebotenen file service gesagt werden.

Bei diesen Punkten erwies sich — und hier darf mal wirklich Microsoft gelobt werden — Windows Server 2003 enterprise edition mal wieder als sehr gutes, robustes und handhabbares Server-Betriebssystem. In der gegebenen Domain-Konfiguration könnte es wohl "locker" die 5 bis 10-fache Last an Konten tragen, und so mehr als die ganze Hochschule Bochum bedienen.

A Anhang

A1. Quellen und Scripte für den laufenden Betrieb

Diejenigen der folgenden Scripte, die währen der Anmeldung werwendet werden befinden sich (auch) repliziert in den entsprechenden "sysvols" der Domain-controller, also z.B. in

```
\\Pd322s\SYSVOL\FB3-MEVA.fh-bochum.de\scripts
```

Anmelde-Script für studentische Nutzer / Seminarkonten

Diese Anmelde-Script muss in der Microsoft-Sprechweise "synchron" laufen. Im Klartext heißt dies ununterbrechbar und nicht nebenläufig mit anderen Start-Threads einer Nutzeranmeldung. Dieser "Synchronlauf" muss auf allen öffentlich zugänglichen Workstations eingestellt sein, er bringt lediglich Nutzen.

```
    24.08.2007 14:53             1.959     studGrup1Anm.bat
---- --------------------  studGrup1Anm.bat  (Anfang)  ---------

@Echo.
D:
S:
@cd \tmp
@Echo.
@chcp 28591
@Echo.
@Echo.
@Echo.
@Echo.
@Echo Anmelde-Skript studGrup1Anm.bat für Seminarkonto %USERNAME%
@Echo V01.04, 24.08.2007, (c) Albrecht Weinert

@REM V01.00    10.10.2005, Albrecht Weinert
@REM V01.02    14.08.2007, Albrecht Weinert: Domain IP reform
@REM V01.03    23.08.2007, Albrecht Weinert: make ownfiles
@REM V01.04    24.08.2007, Albrecht Weinert: conig\firstlog auf Z:

@Echo.
@Echo.
@Echo Nach dem Anmelden mit dem Seminarkonto   "%USERNAME%"
@echo am PC %COMPUTERNAME% folgt nun die Einzelauthentifizierung
für
@echo Ihr persönliches Konto an der Domain FB3-MEVA.
@Echo.
```

```
@Echo.
@Echo.
@REM Echo TEST TEST TEST @REM dir C:\Programme\util\LogAlert.jar
@REM pause

C:\Programme\jdk\bin\java.exe -jar C:\Programme\util\LogAlert.jar
Z: \\193.175.115.4\fb3stud\ -v
@if NOT ERRORLEVEL 4  goto :connP

@REM  echo TEST TEST @pause
@shutdown /l
@Echo.
@Echo Keine solche Anmeldung als %USERNAME% am PC %COMPUTERNAME%.
@Echo.
@goto :stopp

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

@REM change                    v--     this      --v signature to
force firsttime start
set anmeldSignature=%USERNAME%_studGrup1AnmBat240807
@if not exist Z:\config\%USERNAME%First.log  goto :firsttime
findstr %anmeldSignature% Z:\config\%USERNAME%First.log
@if not errorlevel 1 goto :en1

:firsttime
@REM wird mit Muster erstellt @md Z:\config
reg import editpadcuruserreg.reg

java de.a_weinert.apps.Update  -r -nDelEmpty   Y:\zLaufwerkMuster\
Z:\
@rem pause
@echo.

@REM @Echo set mark
Echo %anmeldSignature% > Z:\config\%USERNAME%First.log
pause
@echo.
@Echo ***  Zum ersten Mal Willkommen unter mevaStGrp/%USERNAME%.
@goto :stopp
```

```
:en1
@echo.
@Echo ***  Erneut Willkommen, FB3-MEVA\%USERNAME% am PC
%COMPUTERNAME%.

:stopp
@echo.
@Echo AnmeldeScript, 24.08.2007,  (c) Albrecht Weinert --  Ende
@REM pause
@set anmeldSignature=
@echo.

---- --------------------  studGrup1Anm.bat  (Ende)  ---------
```

Anmelde-Script für andere Nutzer (Kernteam)

Auch diese Script läuft besser "synchon".

```
    15.08.2007  15:25             2.330 homeAnm.bat

---- --------------------  homeAnm.bat  (Anfang)  -----------

@Echo.
@Echo.
@Echo AnmeldeScript homeAnm.bat  f. home/%USERNAME%  Start
@Echo.

@Echo zuletzt modif. am 15.08.2007,  (c) Albrecht Weinert
@Echo wg. Intranetzone-Registries und Renovierung der Domain FB3-
MEVA
@Echo.
@Echo.

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

net use p:    \\PD327S\Programme /persistent:no
if errorlevel 1 goto :noserver
net use z:    \\PD327S\home     /persistent:no
if errorlevel 1 goto :noserver

@echo Der Server PD327S 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 PD327S ist nicht zu erreichen.
@Echo Der Server PD337S 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
PD2327S != PD337S
@echo.

net use p:    \\PD337S\Programme /persistent:no
net use z:    \\PD337S\home     /persistent:no
@echo off

:look1

REM change         v    this                    v signature to
force firsttime start
set anmeldSignature=%USERNAME%homeAnm.bat15.08.07
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
regedit /s editpadcuruserreg.reg
regedit /s zone2.reg
regedit /s zone3.reg
regedit /s wsusMEVA.reg
regedit /s screensavuser.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 (15.08.2007, PD322S.sysvol) f. %USERNAME%
Ende
@set anmeldSignature=
@pause
---- --------------------  homeAnm.bat  (Ende)  -----------
```

Script für File-Server-Backup (Auszug

Dieses Script läuft mindestens einmal täglich (sprich "nächtlich") als Task auf dem Fileserver PD337S. Das Konto für diese Task hat die entsprechenden Rechte auf alle betreffenden Dateibereiche.

```
    23.11.2007  10:14             1.839 backFileServers.bat

---- -------------------- backFileServers.bat (Anfang) -----------
@Echo.
@Echo (--  backFileServers.bat on PD337S,  23.11.2007,  A. Weinert   ---
@Echo.
@set  tmpT=%date:~8,2%%date:~3,2%%date:~0,2%_%time:~0,2%
%time:~3,2%
@set  tmpU=%tmpT: =0%
@echo timeStamp="%tmpU%"  (first start)
@set  rLogFile=D:\logFiles\backFileServers%tmpU%.log
@echo bFlogFile="%rLogFile%" (first task)

@Echo.
```

```
@Echo (- Homeverzeichnisse von  \Pd327s\home\   nach  hier  h:\home\  --
@echo.

robocopy  \\Pd327s\home\  h:\home\ /S /E /B /SEC
                  /A-:RASH /R:2 /W:2 /LOG+:%rLogFile% /NP

@Echo.
@Echo -- Homeverzeichnisse von  \Pd327s\home\   nach  hier
h:\home\  --)
@echo.

@Echo.
@Echo (-- ProgServer   \\pd327s\progserver == hier c:\progserver\  --
@echo.

robocopy  c:\progserver\  \\pd327s\progserver\ /S /E /B /SEC
                         /A-:A /R:2 /W:2 /LOG+:%rLogFile% /NP

robocopy  \\pd327s\progserver\   c:\progserver\
             /S /E /B /SEC /A-:A /R:2 /W:2 /LOG+:%rLogFile% /NP

@Echo.
@Echo -- ProgServer    \\pd327s\progserver == hier c:\progserver   --)
@echo.



@Echo.
@Echo (-- Nutzerverzeichnisse von hier f:\fb3stud\ nach
\\Pd327s\fb3stud\ --
@echo.
@REM Entwicklerhinweis: append nehmen, da logfiles bei Laufzeit <
1min gleich sein können
@set  tmpT=%date:~8,2%%date:~3,2%%date:~0,2%_%time:~0,2%
%time:~3,2%
@set  tmpU=%tmpT: =0%
@echo timeStamp="%tmpU%"  (user files task)
@set  rLogFile=D:\logFiles\backFileServers%tmpU%.log
@echo bFlogFile="%rLogFile%" (user files task)
@echo.
@echo.

robocopy  f:\fb3stud\  \\Pd327s\fb3stud\ /S /MIR /B /SEC
                      /A-:RASH /R:2 /W:2 /LOG+:%rLogFile% /NP
```

```
@Echo.
@Echo - Nutzerverzeichnisse v.hier f:\fb3stud\ nach \\Pd327s\fb3stud\ -)
@echo.



:end
@echo.
@echo.
@echo timeStamp="%tmpU%" (last task start)
@echo bFlogFile="%rLogFile%" (last task)
@echo.
@Echo --  backFileServers.bat (c) Albrecht Weinert  -- on PD337S ------)
@Echo.

---- --------------------  backFileServers.bat (Ende)  -----------
```

A2. Quellen und Scripte für Installation und Wartung

Die folgenden Scripte müssen nur einmalig ausgeführt werden, sei es

- zur bzw. nach der Installation oder
- bei erstmaliger Anmeldung bei dem Rechner

Teilweise lassen sie sich remote ausführen und teilweise verlangen sie lokale Anmeldung z.T. mit administrativen Rechten.

Script für Grundinstallation (remote)

Alle Rechner der Domain FB3-MEVA sollen eine gleiche Grundstruktur an Partitionen Laufwerten und Verzeichnissesn mit festen Rollen haben. Ein Symptom ist, dass bei allen solchen Rechnern die Pfadangabe (path) so

```
PATH=C:\bat;C:\Programme\util;C:\programme\jdk\bin;
      C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem
```

ist oder zumindest so (genau so!) beginnt.

Das folgende Script (mit seinen anschließenden) Hilfsscripts gibt einem betriebssystemmäßig frisch installierten Rechner genau diese Struktur und bereitet die weiterere lokale Installation optimal vor. Es läuft remote auf (genau) einem entsprechend ausgestatteten Domain controller. "Entsprechend ausgestattet" heißt, dass er die Musterverzeichnisstrukturen und -Inhalte sowie die Installationsdateien entsprechend und aktuell vorhält.

Dies "remote" verfahren funktioniert auch für Server, ja sogar für künftige Domain-Controller.

```
21.08.2007  13:32             4.230 baseInstallComputer.bat
-------------------------------------------------------------
```

```
@echo.
@chcp 28591
@echo (------------   baseInstallComputer.bat V0.01 (06.08.2007)
A. Weinert  ---
@echo.
@echo Basis-Installationen für den Computer %1 in der Domain FB3-
MEVA
@echo.
@if %1x==x goto :aufruf
@if /I %1==-help goto :aufruf
@if /I %1==/help goto :aufruf
@if not %1==/?       goto :make

:aufruf
@echo Aufruf:  baseInstallComputer name [-action]
@echo.
@echo Der Computer name bekommt die grundlegenden Installationen
und
@echo und Einstellungen für ein Mitglied der Domain FB3-MEVA.
@echo Dieses Script wird i.A. unmittelbar nach
Systemneuinstallation und/
@echo oder Aufnahme des Computers in die Domain FB3-MEVA auf einem
DC
@echo (PD322s) ausgeführt. Vgl. joinComputerDomain.bat.
@echo.
@echo Optionen:
@echo -makeDirs    phase 1: directories, registries, acls
@echo -fillDirs    phase 2: standard  content,
@echo -all oder entfällt  : alle Phasen
@goto :stopp

:noSuchComputer
@echo no (unique) computer %1 in Active Directory / Domain FB3-
MEVA
@goto :stopp

:isOff
@echo computer %1 is off or not on LAN.
goto :stopp



:make
```

```
@set foundCompi=
@call moveComputerTo %1 Computers
@if  %foundCompi%x==x goto :noSuchComputer
java de.a_weinert.apps.PCon %1 -v
@if ERRORLEVEL 5 goto :isOff
@echo.

@echo computer %1 is on LAN, do ... %2
@echo.

@REM switch mit %2 hier ergänzen
@if %2x==x      goto :makeDirs
@if /I %2==-all goto :makeDirs
@if /I %2==-makeDirs goto :makeDirs
@if /I %2==-fillDirs goto :fillDirs
@echo Ungültige achion - Option
@goto :aufruf

:makeDirs
@echo %1 instalation, phase 1: directories, registries, acls

call makeJederDir.bat  \\%1\C$\temp
call makeJederDir.bat  \\%1\C$\tmp

call makeJederDir.bat  \\%1\D$\temp
call makeJederDir.bat  \\%1\D$\tmp

call makeJederDir.bat  \\%1\S$\temp
call makeJederDir.bat  \\%1\S$\tmp

call makeAdminReadableDir.bat  \\%1\D$\install

md    \\%1\D$\weinert
setacl  \\%1\D$\weinert   /dir  /grant  weinert   /full
/P:no_dont_copy
md    \\%1\D$\seidel
setacl  \\%1\D$\seidel   /dir  /grant  seidel   /full
/P:no_dont_copy
md    \\%1\D$\nowak
setacl  \\%1\D$\nowak   /dir  /grant  nowak   /full
/P:no_dont_copy
```

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

@REM ermöglicht "zweistufige" sichere Anmeldung und ist in jedem
Falle schneller (und sicherer)
reg add  \\
%1\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Po
licies\System\ /v RunLogonScriptSync /t REG_DWORD /d 1 /f

@REM Wert 0 für Anmelden nur mit Domain-Verbindung
reg add  "\\%1\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon" /v CachedLogonsCount /t REG_SZ /d 0 /f

@REM nur für den Lofoff-Screensaver
setacl   "\\%1\MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\IniFileMapping\control.ini"   /registry   /grant
Jeder /create_subkey
setacl   "\\%1\MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\IniFileMapping\control.ini"   /registry   /grant
Jeder /set_val

setx /S %1 TMP S:\TMP /M
setx /S %1 TEMP S:\TEMP /M
setx /S %1 JAVA_HOME C:\Programme\jdk /m
setx /S %1 cvsroot :sspi:PD321S:/cvs/repo /M
setX /S %1 PATH "C:\bat;C:\Programme\util;C:\programme\jdk\bin;
  C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem" /m
setX /S %1 ANT_HOME C:\Programme\Apache\ant /m

@if %2x==x      goto :fillDirs
@if /I %2==-all goto :fillDirs
@goto :stopp

:fillDirs
@echo %1 installation, phase 2: standard directories content,

robocopy C:\c-Laufwerk\bat  \\%1\C$\bat\   /S /E /XO /R:4 /W:6 /NP
```

```
xcopy /y /S C:\c-Laufwerk\programme\*.*    \\%1\C$\programme\

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

xcopy /y C:\C-Laufwerk\config\*.*    \\%1\C$\config\

xcopy /Y C:\C-Laufwerk\desktop\*.*  "\\%1\C$\Dokumente und
Einstellungen\All Users\Desktop\"

xcopy /Y /S C:\C-Laufwerk\install\*.*  "\\%1\D$\install\"

:stopp
@echo.
@echo   ---------   baseInstallComputer.bat (c) A. Weinert ---)

------------------------------------------------------------

07.08.2007  10:16             1.086 makeUserReadableDir.bat
------------------------------------------------------------
@chcp 28591
@echo.
@echo (----- makeUserReadableDir.bat (%1)  V0.01 (06.08.2007) A.
Weinert ---
@echo.
@if not %1x==x goto :make
@echo Parameterfehler!
@echo Aufrufbeispiel:
@echo         makeUserReadableDir  \\PD3Wxyz\C$\bat
@echo.
@Echo Erzeugt angegebenes Verzeichnis mit administrativem
   Vollzugriff und für Domänen-Benutzer: Lesen Ausführen
   Angucken  (ohne Erben)
@echo Anwendungsfälle: gemeinsame Programm- und
   Informationsverzeichnisse
goto :stopp

:make
md %1
setacl  %1   /dir  /grant  Domänen-Admins   /full /P:no_dont_copy
setacl  %1   /dir  /grant  SYSTEM    /full
@REM setacl  %1   /dir  /grant  weinert   /full
setacl  %1   /dir  /grant  Administratoren  /read
```

```
setacl  %1   /dir  /grant  Administratoren  /read_ex
setacl  %1   /dir  /grant  Administratoren  /list_folder
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.
@echo   -- makeUserReadableDir.bat (c)  A. Weinert ------------)

---------------------------------------------------------------
07.08.2007  10:16               873 makeJederDir.bat
---------------------------------------------------------------
@echo.
@chcp 28591
@echo (----- makeJederDir.bat (%1)  V0.01 (07.08.2007) A. Weinert
---
@echo.
@if not %1x==x goto :make
@echo Parameterfehler!
@echo Aufrufbeispiel:
@echo         makeJederDir  \\PD3Wxyz\S$\temp
@echo.
@Echo Erzeugt angegebenes Verzeichnis mit Vollzugriff für
      "Jeder" und einige System-/Admin-Konten (ohne Erben)
      "Jeder" darf das betreffende / erzeugte Verzeichnis
      nicht löschen.
@echo Anwendungsfälle; gemeinsame Log- und Temp-Verzeichnisse
goto :stopp

:make
md %1
setacl  %1   /dir  /grant  Domänen-Admins   /full /P:no_dont_copy
setacl  %1   /dir  /grant  SYSTEM    /full
setacl  %1   /dir  /grant  Jeder   /full
setacl  %1   /dir  /deny  Jeder   /delete /I:no_prop_inh
:stopp
@echo.
@echo       -- makeJederDir.bat (c)  A. Weinert  ---------------)
---------------------------------------------------------------

07.08.2007  10:17               727 makeAdminReadableDir.bat
---------------------------------------------------------------
```

```
@chcp 28591
@echo.
@echo (- makeAdminReadableDir.bat (%1)  V0.01 (06.08.2007) A.
Weinert
@echo.
@if not %1x==x goto :make
@echo Parameterfehler!
@echo Aufrufbeispiel:
@echo         makeAdminReadableDir  \\PD3Wxyz\D$\install
@echo.
@Echo Erzeugt angegebenes Verzeichnis mit Domänen-Admins
       Vollzugriff (ohne Erben) Anwendungsfall:
       Verzeichnisse für nur administrative Aufgaben
goto :stopp

:make
md %1
setacl  %1   /dir  /grant  Domänen-Admins   /full /P:no_dont_copy
setacl  %1   /dir  /grant  SYSTEM    /full
@REM setacl  %1   /dir  /grant  weinert   /full

:stopp
@echo.
@echo  -- makeAdminReadableDir.bat (c)  A. Weinert -----------)
```

Script für Grundinstallation (local)

Wenn die "remote" Grundinstallation gelaufen ist, findet ein lokal angemeldeter Domain-admin die folgenden zwei Scripte (und die Installationsdateien) vor, welche die notwendigste Basis-Softeware auf dem neuen Rechner installieren.

Hinweis: Alle diese Scripte und die auf dem Server bereitgestellten Musterverzeichnisse werden ständig auf den neuesten Stand gebracht und zueinander konsistent gehalten. Was Sie hier als Muster / Anleitung sehen, ist im konkreten Software-Einzelfall (wie unten noch Eclipse 3.2 statt 3.3) schnell veraltet.

```
-------------------------------------------------------------------
20.08.2007  15:54             5.038 LocalInstall.bat
-------------------------------------------------------------------
@Echo (--  LocalInstall.bat  V.01.02  20.08.2007   A. Weinert ---
@echo.
@REM
@REM Dieses Script muss nach .baseInstx, welche auf einem DC
```

```
@REM (PD322S) laufen, auf einem neu einzurichtenden MEVA-Lab-
@REM Rechner lokal laufen.

@chcp 28591
@title Lokale Installationen (Basis, ISO 8859-1)

C:\config\wsusMEVA.reg
C:\config\editpadcuruser.reg

"D:\install\Firefox Setup 2.0.0.2.exe"

D:\install\jdk-6u2-windows-i586-p.exe
del C:\WINDOWS\system32\java.exe
del C:\WINDOWS\system32\javaw.exe

D:\install\AdbeRdr70_deu_full.exe
@echo.
@echo Erst dann eine Taste drücken,
      wenn Acrobat-Installation fertig ist
@pause

@Echo.
@Echo InfranView-Installation
@Echo choose "for all users" !!
@Echo deselect "google search" !!
@echo.
D:\install\iview398.exe
D:\install\irfanview_plugins_400_setup.exe

@Echo.
@Echo installing StarOffice 8 + (pause) one update
@echo.
D:\install\Staroffice\office\setup.exe
@echo.
@echo Erst dann eine Taste drücken,
      wenn Staroffice-Grundinstallation fertig ist
@pause
@Echo.
@Echo installing StarOffice 8 update
@echo.
D:\install\Staroffice\update!\so-8-pp5-bin-windows.exe
@Echo.
@echo.
```

```
@echo Erst dann eine Taste drücken,
      wenn Staroffice-Update fertig ist
@pause

Xcopy /Y "C:\Dokumente und Einstellungen\All
Users\Startmenü\Programme\StarOffice 8\StarOffice Writer.lnk" "C:\
Dokumente und Einstellungen\All Users\Desktop\"
Xcopy /Y "C:\Dokumente und Einstellungen\All
Users\Startmenü\Programme\StarOffice 8\StarOffice Calc.lnk"
"C:\Dokumente und Einstellungen\All Users\Desktop\"
Xcopy /Y "C:\Dokumente und Einstellungen\All
Users\Startmenü\Programme\StarOffice 8\StarOffice Draw.lnk"
"C:\Dokumente und Einstellungen\All Users\Desktop\"
Xcopy /Y "C:\Dokumente und Einstellungen\All
Users\Startmenü\Programme\StarOffice 8\StarOffice Impress.lnk"
"C:\Dokumente und Einstellungen\All Users\Desktop\"



@echo Office shortcuts installieren
@echo
C:\Programme\admTools\Shortcut.exe /F:"C:\Dokumente und
Einstellungen\All Users\Desktop\Word.lnk" /A:C
/T:"C:\Programme\Microsoft Office\Office\WINWORD.EXE"
/W:D:\temp /D:"Word"
C:\Programme\admTools\Shortcut.exe /F:"C:\Dokumente und
Einstellungen\All Users\Desktop\Excel.lnk" /A:C
/T:"C:\Programme\Microsoft Office\Office\EXCEL.EXE"  /W:D:\temp
/D:"Excel"
C:\Programme\admTools\Shortcut.exe /F:"C:\Dokumente und
Einstellungen\All Users\Desktop\Powerpoint.lnk" /A:C
/T:"C:\Programme\Microsoft Office\Office\POWERPNT.EXE"  /W:D:\temp
/D:"PowerPnt"
C:\Programme\admTools\Shortcut.exe /F:"C:\Dokumente und
Einstellungen\All Users\Desktop\PhotoEdit.lnk" /A:C
/T:"C:\Programme\Gemeinsame Dateien\Microsoft
Shared\PhotoEd\PHOTOED.EXE"  /W:D:\temp /D:"PhotoEdit"


del "C:\Dokumente und Einstellungen\All Users\Startmenü\Neues
Office-Dokument.lnk"
del "C:\Dokumente und Einstellungen\All Users\Startmenü\Office-
Dokument öffnen.lnk"


del "C:\Dokumente und Einstellungen\All Users\Startmenü\Programme\
Autostart\Adobe Reader - Schnellstart.lnk"
del "C:\Dokumente und Einstellungen\All Users\Startmenü\Programme\
Autostart\Microsoft Office.lnk"
```

```
del "C:\Dokumente und Einstellungen\All Users\Startmenü\Programme\
Zubehör\Remotedesktopverbindung.lnk"
del "C:\Dokumente und Einstellungen\All Users\Startmenü\Programme\
Zubehör\WordPad.lnk"
del "C:\Dokumente und
Einstellungen\admin\Startmenü\Programme\Zubehör\Editor.lnk"
del "C:\Dokumente und
Einstellungen\admin\Startmenü\Programme\Zubehör\Adressbuch.lnk"
del "C:\Dokumente und
Einstellungen\admin\Startmenü\Programme\Zubehör\Programmkompatibil
itäts-Assistent.lnk"

del "C:\Dokumente und Einstellungen\Default
User\Startmenü\Programme\Zubehör\Editor.lnk"
del "C:\Dokumente und Einstellungen\Default
User\Startmenü\Programme\Zubehör\Synchronisieren.lnk"
del "C:\Dokumente und Einstellungen\Default
User\Startmenü\Programme\Zubehör\Programmkompatibilitäts-
Assistent.lnk"
del "C:\Dokumente und Einstellungen\All Users\Startmenü\Programme\
Microsoft Access.lnk"
del "C:\Dokumente und Einstellungen\All Users\Startmenü\Programme\
Microsoft Excel.lnk"
del "C:\Dokumente und Einstellungen\All Users\Startmenü\Programme\
Microsoft Word.lnk"
del "C:\Dokumente und Einstellungen\All Users\Startmenü\Programme\
Microsoft PowerPoint.lnk"

:stopp
@chcp 850
@title DOS-Shell (CP 850)
@echo.
@echo.
@Echo Neu starten und mit LocalInstallStep2 fortfahren.
@echo.
@Echo   ---------  LocalInstall.bat  (c) A. Weinert ------)

-----------------------------------------------------------------
01.09.2007  11:50             1.814 LocalInstallStep2.bat
-----------------------------------------------------------------
@Echo (-- LocalInstalStep2.bat  V.01.01 20.08.2007  A. Weinert ---
@echo.
@REM Dieses Script muss nach LocalInstal.bat und Neustart
@REM auf einem neu einzurichtenden MEVA-Lab-Rechner lokal laufen.
```

```
@chcp 28591
@title Lokale Installationen; Schritt 2 nach Neustart   ISO 8859-1

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

del C:\WINDOWS\system32\java.exe
del C:\WINDOWS\system32\javaw.exe

cd /D C:\programme\jdk

jar xfv D:\install\jdk-6-doc.zip
jar xfv D:\install\erg.zip
java ShowPorts
java ShowProps

cd /D C:\programme
@REM      file is Eclipse3.2 Java + Web develop.
jar xfv   D:\install\wtp-all-in-one-sdk-R-1.5.0-200606281455-
win32.zip
@echo.
@Echo Eclipse first time
@Echo choose D:\eclipseWS as workspace !!
@echo.
C:\Programme\eclipse\eclipse.exe

C:\Programme\admTools\Shortcut.exe /F:"C:\Dokumente und
Einstellungen\All Users\Desktop\Eclipse32.lnk" /A:C
/T:C:\Programme\eclipse\eclipse.exe  /W:D:\eclipseWS /D:"Eclipse
3.2 wtp"

@goto :stopp

@REM ausgeblendet, da bereits remote installiert:

:setSysVar
@echo Setzen der Systemvariablen TMP, TEMP, JAVA_HOME und PATH-
Erg. (einmalig)
setx TMP S:\TMP /M
setx TEMP S:\TEMP /M
```

```
setx JAVA_HOME C:\Programme\jdk /m
setx cvsroot :sspi:PD321S:/cvs/root /M
setX PATH "PATH=C:\bat;C:\Programme\util;C:\programme\jdk\bin;;C:\
WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem" /m
setX ANT_HOME=C:\Programme\Apache\ant /m
:sysVarSet


:stopp
@chcp 850
@title DOS-Shell (CP 850)
@echo.
@Echo    ---------  LocalInstalStep2.bat  (c) A. Weinert ------)

-----------------------------------------------------------------
```

Registry-Script für Benutzbarkeit von Netzfreigaben im Dateiexplorer

Scripte wie dieses sind nur notwendig, da Microsoft Datei-Befehle (Xcopy, Del, ren etc.) anders behandelt als entsprechende Maustaten im Explorer. Bei letzteren wirken zusätzlich zu den dafür ja zuständigen und bestens geeigneten NTFS-Dateirechten (ACLS) Sicherheitsbremsen, die man mit dem Internet-Explorer verwaltet.

Die Scripts beseitigen diesen aus Dateiexplorer-Nutzersicht unverständlichen Blödsinn weitestgehend. Es muss pro user-Profil (erste Anmeldung / Bereitstellung eines serverbasierten festen Profils) einmal laufen.

Hinweis 1: zone2.reg ist für alle Nutzer; es gibt noch ein ähnliches Registry-Script mit weiteren Einträgen für priviligiertere Nutzer.

Hinweis 2:

```
     ::::::::
```

bedeutet Fortsetzung mit fortlaufender Benennung / Nummerierung der Rechner.

```
    15.08.2007  09:16             2.722 zone2.reg
---- -----------------------------------
Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Inter
net Settings\ZoneMap\EscDomains\pd321s]
"file"=dword:00000001
"http"=dword:00000001
"https"=dword:00000001

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Inter
net Settings\ZoneMap\EscDomains\pd322s]
"file"=dword:00000001
```

```
     ::::::::  pd322s ..  pd324s

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Inter
net Settings\ZoneMap\EscDomains\pd324s]
"file"=dword:00000001

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Inter
net Settings\ZoneMap\EscDomains\pd310s]
"file"=dword:00000001
"http"=dword:00000001
"https"=dword:00000001

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Inter
net Settings\ZoneMap\EscDomains\pd3022]
"file"=dword:00000001

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Inter
net Settings\ZoneMap\EscDomains\pd3023]
"file"=dword:00000001

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Inter
net Settings\ZoneMap\EscDomains\netdrive]
"file"=dword:00000001

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Inter
net Settings\ZoneMap\EscDomains\pd313d]
"file"=dword:00000001

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Inter
net Settings\ZoneMap\EscDomains\pd3091]
"file"=dword:00000001---- ------------------------------------
```

Registry-Script für WSUS (FH)

Dies Script schließt einen Rechner an den Firmen (hier FH-) Server für Windows-Update an. Die hier gezeigten Einstellungen geben automatisches Laden, aber ggf. administratorgeführte Installation vor (hat sich bewährt).

```
   17.11.2005  11:09             1.010 wsusMEVA.reg
---- ------------------------------------

Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\windows\WindowsUpd
```

```
ate]
"WUServer"="http://pc0022"
"WUStatusServer"="http://pc0022"

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\windows\WindowsUpd
ate\AU]
"NoAutoUpdate"=dword:00000000
"AUOptions"=dword:00000003
"ScheduledInstallDay"=dword:00000000
"ScheduledInstallTime"=dword:00000003
"RescheduleWaitTime"=dword:00000012
"NoAutoRebootWithLoggedOnUsers"=dword:00000001
"UseWUServer"=dword:00000001
---- ----------------------------------------
```

Script für "synchrone Anmeldung"

Dieses Script stellt einen Rechner (der Domain) auf das "synchrone Anmeldeverfahren" um, das in jeder Hinsicht besser (schneller, sicher) ist. Mit administrativer Anmeldung lässt es sich remote ausführen, auch in einer Schleife. Der Anschaltzustand des betr. Rechners wird geprüft.

Zusätzlich setzt es Rechte in der Registry, die wegen eines Bugs des Microsoft-Logoffscreensavers verlangt werden.

```
  21.08.2007  10:26             1.077 makeLogOnSync.bat
---- ------------------------------------
```

```
@echo.
@echo (--  makeLogOnSync.bat V01.00 (21.08.2007) A. Weinert    --
@REM  V0.00 (24.03.2006 12:04) A. Weinert
@echo.
@echo makeLogOnSync %
@echo.
@if not %1x==x goto :make
@echo Parameterfehler!
@echo Aufrufbeispiel:
@echo      makeLogOnSync  PD3W701
goto :stopp

:isOff
@echo computer %1 is off or not on LAN.
goto :stopp
```

```
:make
java de.a_weinert.apps.PCon %1 -v
@if ERRORLEVEL 5 goto :isOff
@echo.

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

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



:stopp
@echo.
@echo ---------   makeLogOnSync.bat V01.00 (c) A. Weinert    ----)
@echo.

---- ----------------------------------------
```

A3. Abkürzungen

ACL	access control list (Liste mit Zugriffsrechten auf ein Objekt)
AD	Active Directory (Microsofts Interpretation von LDAP)
AJAX	Asynchronous JavaScript + XML
API	Application Programme Interface
BuB	Bedienen und Beobachten (von Prozessen)
C/S	Client-Server
CA	Certification authority
CIP	Computer-Investitions-Programm (der Landesregierungen; i.A. für studentische Arbeitsplätze an Hochschulen); im NEVA-Lab:Computer Intelligence Pool
FAQ	Frequently Asked Questions (Hilfetexte in Frage-Antwort-Form)
FB	Fachbereich; insbesondere ...

FB3 Fachbereich Elektrotechnik und Informatik der FH Bochum

FH Fachhochschule

GSS Generic Security Service

GUID Globally Unique Identifier

GWT Google Webtoolkit, AJAX mit nur Java

HISS Hochschulinformationssystem o.ä.

HTML Hypertext Markup Language [RFC 1866]

HTTP Hypertext Transfer Protokoll.
Internet-Protokoll zur Übertragung von Seiten.

HTTPS HTTP über SSL. Abgesicherte Übertragung.

HW Hardware

IIOP Internet Inter-ORB Protocol

IP Internet Protocol

J2EE Java 2 Enterprise Edition

J2ME Java 2 Micro Edition

J2SE Java 2 Standard Edition

JAAS Java Authentication and Authorization Service

JAF JavaBeans Activation Framework

JAR Java Archive. (.zip + Semantik)

JAXP Java API for XML Parsing

JCA Java Cryptography Architecture (der Java Security API)

JCE Java Cryptography Extensions (zur JCA, Exportrestriktion wegen DAS, DES)

JDBC Java Database Connectivity (Java Datenbankanschluss)

JDC Java Developer Connection (Ein WWW-Service)

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

JEB Enterprise JavaBeans (ungleich JavaBeans)

JMX Java Management Extensions

JNDI Java Naming and Directory services Interface

JNI Java Native Interface

JRE Java Runtime Environment; JDK-Subset ohne Entwicklungswerkzeuge.

JSDK Java Servlet Development Kit

JSF Java Server Faces

JSP Java Server Pages

JSSE Java Secure Socket Extension (seit JDK1.4.x integriert)

JSTL JavaServer Pages Standard Tag Library

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

LAN Local area network; Datennetz für mittlere Entfernungen

LDAP Lightweight Directory Access Protocol

LGPL Lesser GNU Public License

MBean Managed Bean (JMX)

MEVA Labor für Medien und verteilte Anwendungen

MS Microsoft

NT Betriebssystem Windows NT (MS)

OMG Object Management Group

OS Operating System

PAM Pluggable Authentication Module

PC Personal Computer

R&D Research and Development

RAID Redundant Array of inexpensive Disks

RDF Resource Description Framework (W3C)

RMI Remote Method Invocation

RPC Remote Procedure Call

SAAJ SOAP with Attachments API for Java

SID security identifier;
eindeutige Identifizierungsnummer für Rechner- Personen- und andere Konten

SMTP Simple Mail Transfer Protocol

SOAP Simple Object Access Protocol

SQL Structured query language, Datenbankbearbeitungssprache

SSL Secure Socket Layer. Protokollschicht zu Absicherung.

SSO Single Sign on; Authentifizierung vieler (n) Anwendungen gegen eine (1) "security realm".
(Stufe1) + (Stufe 2) nur einmaliges Anmelden für viele Anwendungen

TCP Transmission Control Protocol

TM Trade Mark (Warenzeichen)

UAA Universal Audio Architecture (intel Erfindung; ab SP2 in W2K3)

UML Unified Modelling Language

URI Uniform Resource Locator

W2K Betriebssystem Windows 2000 (MS)

W2K3 Betriebssystem Windows Server 2003 (MS)

W3 Amerikanische Kurzform für WWW

W3C World Wide Web Consortium

WS Workstation

WSDL Web Services Description Language

XML eXtensible Markup Language

A4. Literatur

[1] Ed Ort and Mark Basler, AJAX Design Strategies, SUN 2006
http://java.sun.com/developer/technicalArticles/J2EE/AJAX/.../design-strategies.pdf

[2] Brett McLaughlin, Mastering Ajax, Part 1..4, IBM, 2005
http://www-128.ibm.com/developerworks/web/library/wa-ajaxintro.html

[3] Albrecht Weinert, Zur Installation des JDK (Java Development Kit)
http://a-weinert.de/weinert/pub/java-install.txt

[4] Albrecht Weinert, Java — Tipps und Tricks
http://a-weinert.de/weinert/pub/java-tips.txt

[5] Albrecht Weinert, AJAX mit GWT — Tipps und Tricks
http://a-weinert.de/weinert/pub/gwt-tips.pdf

[6] Albrecht Weinert, Tipps zu CVS für Windows — cvsNT
http://a-weinert.de/weinert/pub/cvsnt-tipp.txt

[7] Google, Web-Toolkit, online-Dokumentation (nicht am Stück verfügbar)
http://code.google.com/webtoolkit/documentation/

[8] Albrecht Weinert, Tipps zu JMX mit SSL
http://a-weinert.de/weinert/pub/jmx-ssl-tips.pdf

[9] Albrecht Weinert, Windows 2003 Domain
Migration von NT4 mit Fremd-DNS
http://www.a-weinert.de/weinert/pub/w2k3domain.pdf

<10> Albrecht Weinert, Windows Server 2003 — Domain FB3-MEVA
Schulungsräume und Infrastruktur — Renovierung 2007
http://www.a-weinert.de/weinert/pub/fb3-meva-domain2007.pdf

[11] Albrecht Weinert, Tipps zu Tomcat (für Windows)
http://a-weinert.de/weinert/pub/tomcat-tips.pdf

[12] Albrecht Weinert, Windows Server 2003 — Domain FB3-MEVA
Workstations und Server — Renovierung 2007
http://www.a-weinert.de/weinert/pub/fb3-meva-workst2007.pdf

Hinweis: Aus Dateien „.../docu/*.txt“ könnten inzwischen teilweise „.../weinert/pub/*.pdf “ geworden sein.