

inforum

INFormationsforum des Rechenzentrums der Universität Münster

Jahrgang 22, Nr. 3 – Oktober 1998

ISSN 0931-4008

Inhalt

Editorial	2
RUM-Aktuell	
Zentrale Servicestelle im ZIV	3
ADSL-Pilotprojekt Münster	3
Vom häuslichen Rechner ins Hochschulnetz	4
Problemanalyse im WWW	5
Selbstanmeldung über das WWW	6
Neue deutsche Rechtschreibung in Textverarbeitungsprogrammen	6
Terminal Server an der WWU	8
Dank für treue Dienste	8
Nutzung des ADSM in der WWU	9
Sicherheitsaspekte beim Einsatz von ADSM	11
Fingerabdrücke	13
Geplante Neubeschaffungen im Unix-Server-Bereich	15
Aktuelles zu SPSS und SAS	16
Planeten, pv~wave und mpeg-movies	17
Nutzung der hochschulweit angebotenen Literaturdatenbanken	19
RUM-Tutorial	
Vertrauen ist gut, Kontrolle ist besser (1)	21
RUM-Lehre	
Lehrveranstaltungen im Wintersemester 1998/99	32



Impressum

inforum

ISSN 0931-4008

Westfälische Wilhelms-Universität
Zentrum für Informationsverarbeitung (Universitätsrechenzentrum)
Röntgenstr. 9 – 13
48149 Münster

E-Mail: ziv@uni-muenster.de

WWW: <http://www.uni-muenster.de/URZ/>

Redaktion: W. Bosse (☎ 83-31561, ✉ bosse@uni-muenster.de)
R. Perske (☎ 83-31582, ✉ perske@uni-muenster.de)
H. Pudlatz (☎ 83-31672, ✉ pudlatz@uni-muenster.de)
E. Sturm (☎ 83-31679, ✉ sturm@uni-muenster.de)

Satzsystem: Corel WordPerfect 8.0 für Windows 95/NT

Druck: Universitätsrechenzentrum
(Rank Xerox DocuTech 135)

Auflage dieser Ausgabe: 1500

Editorial

E. Sturm



Es ist so weit! Während sich andere Zeitungen und Zeitschriften noch auf den Standpunkt stellen: Wir ziehen nach, wenn die Nachrichtenagenturen umgestellt haben, „bemühen wir uns um die Verwirklichung der neuen Rechtschreibung“, wie es in einem Brief des Rektorats an alle Beschäftigten der Westfälischen Wilhelms-Universität heißt. Wir wiederholen ja auch nicht die Nachrichten anderer, wir machen unsere Nachrichten selbst!

Für die Bezieher des **inforum** in Schleswig-Holstein tut es mir leid. Auch nach dem Volksentscheid sehen wir uns nicht in der Lage, zusätzlich eine Ausgabe in alter Rechtschreibung auszuliefern.

Auf dem Schreibtisch liegt jetzt immer ein Wörterbuch, damit wir nicht im Dunkeln tappen, ob wir „im Allgemeinen“ im Folgenden tatsächlich groß schreiben sollen. Die Textverarbeitungssysteme haben, wie Sie in diesem **inforum** lesen können, auch noch so ihre Schwierigkeiten.

Natürlich ist nicht Rechtschreibung Thema dieses Heftes. Wie immer geht es hauptsächlich um Vernetzung: Wir spannen einen Bogen von ADSL über ADSM, DCE, ISDN und PGP bis zum WWW. Apropos WWW: Für dieses **inforum** verschicken wir zum ersten Mal per E-Mail eine Ankündigung an Benutzer, die sich bereit erklärt haben, auf eine Papierversion zu verzichten. In der Ankündigung wird per „Link“ direkt auf jeden Artikel im WWW verwiesen. Wenn Sie es ihnen gleich tun wollen, benutzen Sie entweder die letzte Seite dieses Heftes (Papier!) oder schicken Sie den Wunsch an inforum@uni-muenster.de!

RUM-Aktuell

Zentrale Servicestelle im ZIV

W. Held

**3 16 00 –
die zentrale Service-
Nummer des ZIV**

Am 02.11.1998 wird im Zentrum für Informationsverarbeitung (Universitätsrechenzentrum) zur Verbesserung der Erreichbarkeit eine zentrale Servicestelle eingerichtet werden: Bitte nutzen Sie dazu möglichst die elektronische Post oder das Telefon:

E-Mail: ziv@uni-muenster.de

Telefon: (02 51) 83-3 16 00

Telefax: (02 51) 83-3 15 55 (nicht im direkten Zugriff der Servicestelle)

Diese Servicestelle ist montags bis freitags von 7.30 Uhr bis 17.30 Uhr durchgehend besetzt. Unsere Nutzer werden gebeten, sich mit allen Themen (Fehlermeldungen, Fragen usw.) zunächst an diese Stelle zu wenden, wenn nicht eine Mitarbeiterin oder ein Mitarbeiter direkt erreicht werden soll.

Die Mitarbeiterin oder der Mitarbeiter in der Anlaufstelle wird einen Teil der Anfragen unmittelbar beantworten können. In allen anderen Fällen sorgt sie/er dafür, dass die zuständigen Spezialisten zur Lösung der vorgetragenen Probleme eingeschaltet werden.

Wichtiger Hinweis:

Sie können zur Entlastung der Mitarbeiterinnen und Mitarbeiter im Zentrum für Informationsverarbeitung entscheidend beitragen, wenn Sie sich zunächst auch über die WWW-Seiten des Zentrums für Informationsverarbeitung um eine Lösung bemühen. Denn bedenken Sie bitte: Wir haben zur Zeit etwa 30.000 Nutzer, die Tendenz ist steigend. Wenn jeder Nutzer uns im Monat nur eine Minute in Anspruch nimmt, belegt das über drei Mitarbeiter/innen. Schauen Sie also zuerst in unser Web:

<http://www.uni-muenster.de/URZ/>

Sie werden dort viele Fragen beantwortet finden, unter anderem können Sie über Stichwörter Hilfe suchen unter

<http://www.uni-muenster.de/exec/Queryindex/URZ>

Wir weisen auch darauf hin, dass Sie sich mit Fragen und Problemen zunächst an Ihre lokale IV-Versorgungseinheit wenden können.

ADSL-Pilotprojekt Münster

W. Held

Schnelle Datenübertragung zum häuslichen Arbeitsplatz

ADSL (*Asymmetric Digital Subscriber Line*) ist ein Kommunikations-Verfahren, mit dem über einfache Telefonleitungen Daten mit hoher Geschwindigkeit übertragen werden können, und zwar mit einer Geschwindigkeit von 8 Mbit/s zum Endnutzer und mit 768 Kbit/s in umgekehrter Richtung. Da Telefonleitungen weit verbreitet sind, ist ADSL ein ganz wichtiges Verfahren, um das Übertragungsproblem der sogenannten letzten Meile zu lösen.

Einen ersten Bericht gaben wir in **inforum** Nr. 4/1997, wo der Anschluss eines münsterischen Studentenwohnheims über ADSL beschrieben wurde. Als allgemeine Einführung in die ADSL-Technik empfehlen wir im WWW den Artikel

<http://www.uni-muenster.de/URZ/ADSLProjekt/ADSLProjekt.html>

und speziell zum „letzten Stand der Dinge“ den Bericht

<http://www.uni-muenster.de/URZ/ADSLProjekt/Status0798.html>

Uni@home



Vom häuslichen Rechner ins Hochschulnetz

Kooperationsprojekt Universität Münster – Deutsche Telekom

W. Held

Schon im Studium kommt es auf die richtigen Kontakte an. Wer mehr weiß und besser erreichbar ist, macht sich das Leben leichter.

Für viele Studierende und Wissenschaftler ist der Zugang vom häuslichen Arbeitsplatzrechner zum Datenkommunikationsnetz der Universität Münster und zum Internet von immer größerer Bedeutung.

Schließlich lassen sich auf diesem Weg viele Arbeiten schnell und leicht erledigen. So können Wissenschaftler von zu Hause aus Abläufe auf den DV-Anlagen des Institutes steuern und kontrollieren. Aber auch die bequeme Nutzung von Netzanwendungen für Forschungsaufgaben wie die Recherche in Wissenschaftsdatenbanken oder die Fernkooperation mit in- und ausländischen Wissenschaftlern auch unter Nutzung gemeinsamer Datenbestände sind damit möglich.

Für die Studierenden ergeben sich ebenfalls viele Vorteile. So setzt die Ausbildung in zunehmendem Maß auf die Nutzung von Rechnern, während die Anzahl der verfügbaren Arbeitsplätze in den Computer-Pools der Universität dem steigenden Bedarf aus finanziellen und Raumnotgründen nicht mehr gerecht werden kann. Der häusliche Arbeitsplatzrechner mit Zugang zum Hochschulnetz ermöglicht es, diese Aufgaben durchzuführen – ohne lange Wartezeiten.

Aber auch andere für das Studium wichtige Arbeiten lassen sich damit leicht und bequem von zu Hause aus durchführen: sei es eine Recherche mittels Suchmaschine im Internet, der Zugriff auf Vorlesungsverzeichnisse und Prüfungsordnungen oder auch die Nutzung der Informationsdienste von Bibliotheken.

Das Zentrum für Informationsverarbeitung (Universitätsrechenzentrum) bietet deshalb den Studierenden und Wissenschaftlern der WWU einen entgeltfreien Zugang zum Internet – nur die Telefonkosten sind selbst zu tragen. Viele nutzen diese Dienstleistung bereits für Studium und Forschung, und täglich werden es mehr. Der Ansturm auf die Einwahlzugänge führt bisher regelmäßig zu Überlastungen der derzeit vorhandenen Anschlüsse.

Das Kooperationsmodell Uni@home der Deutschen Telekom und der Universität Münster soll hier Abhilfe schaffen, besetzten Leitungen endgültig ein Ende bereiten und damit den Dienst zuverlässiger werden lassen. Die Deutsche Telekom hat im Rahmen des Projektes Uni@home der Universität Münster Leitungen und Netzzugangstechnik unentgeltlich zur Verfügung gestellt und dadurch die Anzahl der Zugänge zum Uni-Netz verdreifacht. Sobald die Anschlusspunkte einen gewissen Auslastungsgrad erreicht haben, wird ihre Anzahl automatisch erhöht. Bei der Anwahl sollte das Besetztzeichen also praktisch nicht mehr ertönen.

Uni@home ist gestartet worden und alle Studierenden und Wissenschaftler der Westfälischen Wilhelms-Universität Münster können das Angebot vom 01.10.1998 an voll nutzen, wobei bei geplanter ISDN-Nutzung der Bereitstellungspreis für einen ISDN-Anschluss (bei Selbstmontage) noch vergütet wird. Und neu ist, dass für Berechtigte, z. B. schwerbehinderte oder GEZ-befreite Studierende, der T-ISDN-Anschluss über die Verbindungspreise als „Sozialanschluss“ überlassen wird. Das Uni-Netz kann natürlich auch über Modem-Verbindungen erreicht werden.

Die Beauftragungen zu den Angeboten Uni@home erfolgen über einen speziellen Vordruck, der in den T-Punkten der Telekom in Münster, Domplatz 6-7 oder Salzstr. 14-15, erhältlich ist. Dort liegen auch Informationsbroschüren aus. Weiterhin wird in den nächsten Tagen an allen bekannten Verteilstellen der Universität Münster Info-

Material mit Bestellmöglichkeit zum Kooperationsmodell erhältlich sein. Selbstverständlich findet jeder Interessent alle Hinweise zu Uni@home – bis zum Herunterladen des Bestellvordruckes – auf einem Server der Telekom mit der Adresse

<http://193.158.123.90/>

Für Rückfragen steht Ihnen das Telekom-Team in den genannten T-Punkten zur Verfügung. Schauen Sie auch in die Web-Seiten des Zentrums für Informationsverarbeitung, dort finden Sie viele technische Informationen. Sie können sich auch an unsere Benutzerberatung in der Einsteinstr. 60 (☎ 3 15 86, 📧 ziv@uni-muenster.de) oder an das DaWIN-Team (☎ 3 16 99, 📧 dawin@uni-muenster.de) wenden, das regelmäßig Einführungsveranstaltungen zu vielen Themen der Datenverarbeitung anbietet. Selbstverständlich steht Ihnen ab dem 02.11.1998 auch unsere zentrale Servicestelle zu Verfügung (s. Seite 3 dieser Ausgabe).

Studierende und Mitarbeiter/innen benötigen zur Nutzung dieser Dienste eine Nutzungsberechtigung. Diese wird Studierenden jeweils in den ersten Semesterwochen automatisch angeboten (s. auch den Artikel „Selbstanmeldung über das WWW“ auf Seite 6). Sie muss von allen anderen, die noch keine Berechtigung haben, beantragt werden. Das Formblatt erhalten Sie im Gebäude Einsteinstraße 60 des Zentrums für Informationsverarbeitung oder im WWW unter

<http://www.uni-muenster.de/URZ/Organisation/Beantragung.html>

Die Telefonnummer für den Einwähldienst lautet 8 80 77 50.

Technische Eigenschaften dieses Dienstes finden Sie unter

[http://www.uni-muenster.de/URZ/Rechnernetz/
EinwahlTechInfo.html](http://www.uni-muenster.de/URZ/Rechnernetz/EinwahlTechInfo.html)

Problemanalyse im WWW

R. Perske

Bei vielen Problemen mit Login, Passwort, E-Mail, NetNews, WWW usw. können Sie sich jetzt selbst helfen oder wenigstens herausfinden, was los ist.

Eine der häufigsten Anfragen an das Zentrum für Informationsverarbeitung (ZIV) lautet: „Können Sie mir helfen? Ich habe Probleme mit meiner E-Mail.“ Oder: „Ich komme nicht mehr rein.“ In solchen Fällen kommen viele sehr unterschiedliche Ursachen in Betracht: Fehler auf Seiten des Nutzers genauso wie Fehler im System.

Um schneller helfen zu können, haben wir die vielen verschiedenen Schritte der Problemanalyse automatisiert und in Form einer WWW-Seite zugänglich gemacht. Das hinter der WWW-Seite steckende Programm wird ständig erweitert und überprüft nicht nur viele verschiedene Fehlermöglichkeiten, sondern ist sogar in der Lage, manchen Fehler selbständig oder auf Aufforderung sofort zu beseitigen, ohne dass ein Mitarbeiter eingreifen muss. Bei anderen Fehlern kann es zumindest die Ursache feststellen, so dass die Mitarbeiter gezielter und schneller helfen können.

Diese WWW-Seite ist nicht nur für die Mitarbeiter gedacht: Sie können und sollten wenn möglich die WWW-Seite sogar selbst aufrufen. Sie finden sie auf der WWW-Titelseite des ZIV unter dem Stichwort „Hilfe, es tut nicht!“ oder direkt unter der WWW-Adresse:

<http://user.uni-muenster.de/exec/help>

Gerade nachts und am Wochenende kann Ihnen die WWW-Seite zumindest in manchen Fällen sofort helfen, so dass die Wartezeit auf den nächsten Dienstbeginn des ZIV entfällt, in den meisten anderen Fällen kann sie Ihnen und uns zumindest mitteilen, wo das Problem liegt.

Selbstanmeldung über das WWW

K.-B. Mertz

Für die Studierenden der WWU wird jeweils am Beginn eines Semesters ein vereinfachtes Anmeldeverfahren zur Benutzung der Rechner des Zentrums für Informationsverarbeitung (ZIV) über unsere WWW-Seiten angeboten.

Alle Studierenden der WWU können ihre Anmeldungen zur Benutzung der Rechner des ZIV vom 21.09.98 bis zum 15.11.98 auch selbst durchführen! Benutzen Sie dazu einen beliebigen Rechner mit Internet-Anschluss und WWW-Browser (z. B. Netscape Navigator) und wählen Sie im WWW die Seite

`http://user.uni-muenster.de/`

Folgen Sie dort dem Link „Anmeldung“. Geeignete Rechner finden Sie in allen CIP-Pools der Universität, z. B. im 1. Obergeschoss des Gebäudes Einsteinstr. 60.

Hinweis für Neuimmatrikulierte des WS 1998/99

Für die Anmeldung zur Benutzung der Rechner des ZIV werden die bei der Immatrikulation abgegebenen persönlichen Daten in maschinenlesbarer Form benötigt. Diese werden uns vom Studierendensekretariat der WWU zur Verfügung gestellt, das aber für die Datenaufnahme einige Zeit benötigt. Die Bearbeitung Ihrer Anträge bzw. die Anmeldung über das WWW ist daher in der Regel frühestens 3 bis 4 Wochen nach der Immatrikulation möglich.

Für welche Matrikelnummern uns die Daten vorliegen, wird im WWW über einen Link von der oben genannten Seite sowie durch Aushang im ZIV bekanntgegeben.

Neue deutsche Rechtschreibung in Textverarbeitungsprogrammen

H. Pudlatz

Nach ersten zaghaften Versuchen im inforum Nr. 1/1995 bemühen wir uns ab sofort, die neue deutsche Rechtschreibung („NDR“) konsequent anzuwenden, und geben Tips für deren Nutzung in Ihrer Textverarbeitung.

Seit 1. August 1998 ist die neue deutsche Rechtschreibung („NDR“) in Behörden und an Schulen Norm. Die Lehrer sind gehalten, diese zu lehren, aber die alte Schreibung noch zu tolerieren. Dies gilt bis zum Jahre 2005.¹ Eine verbindliche Durchführungsrichtlinie des MSWWF (also des neuen NRW-Ministeriums für Schule und Weiterbildung, Wissenschaft und Forschung) steht noch aus, die Mitteilung Nr. 4/1998 der Zentralen Universitätsverwaltung empfiehlt aber, im Vorgriff auf eine solche Richtlinie die NDR einheitlich in allen offiziellen Mitteilungen (also auch bei wissenschaftlichen Publikationen!) zu verwenden.

Soweit man sich hierbei der automatisierten Textverarbeitung bedienen kann, sollte man erwarten, dass eine Hilfestellung vom verwendeten Textverarbeitungssystem angeboten wird. Diese ist jedoch unterschiedlich realisiert. Ich will hier nur die am häufigsten im Universitätsbereich genannten Systeme betrachten:

Corel WordPerfect 8.0 für Windows 95 / NT

Dieses Textverarbeitungsprogramm verwenden wir auch beim inforum-Satz. Von WordPerfect ist man gewohnt, dass es bei eingeschalteter Rechtschreibprüfung die nicht im Wörterbuch enthaltenen Wörter rot unterstreicht bzw. bei eingeschalteter Blitzkorrektur auch korrigiert, was allerdings manchmal zu kuriosen Verbesserungsvorschlägen führt (Das „Internet“ kann da leicht zum „Internat“ werden!).

Seit der Version 8.0 werden die alte und die neue Rechtschreibung parallel unterstützt.

¹ Der Volksentscheid vom 27.9.1998 in Schleswig-Holstein dürfte daran kaum etwas ändern, zumal von offizieller Stelle verlautet, dass dort künftig beide Schreibweisen akzeptiert werden.

Bei der Installation werden beide Wörterbücher installiert. Beim ersten Start des Programms hat man die Auswahl zwischen drei Alternativen:

- alte Rechtschreibung
- neue Rechtschreibung
- beide Rechtschreibsysteme sind zugelassen

Sinnvollerweise wird man sich für die eine oder andere Schreibung aber nicht für beide gleichzeitig entscheiden, denn was macht es für einen Eindruck, wenn man in einem Dokument einmal „daß“ und ein andermal „dass“ schreibt, ohne dass das System dies moniert? Wir haben uns also für die NDR entschieden.

Will man in einer neuen WP-Sitzung allerdings mal wieder die alte Schreibweise benutzen, so kann das verwendete Wörterbuch gewechselt werden durch die Menübefehle *Tools - Rechtschreibprüfung - Optionen - Hauptwortlisten - Alte Rechtschreibung*. Die alten Regeln gelten dann ab dem Neustart des Programms für die folgenden Sitzungen, da das Wörterbuch beim Programmstart fest zugeordnet wird. Dies gilt so lange, bis über die analoge Befehlssequenz die neuen Regeln für die nächste Sitzung wieder wirksam gemacht werden.

Word für Windows 97

Die aktuelle Version des Textverarbeitungssystems von Microsoft zeigt momentan leider weniger Flexibilität: Hier gilt zunächst noch die alte Schreibung. Es wird aber ein Wörterbuch angeboten, das beide Schreibweisen toleriert (der Sinn dieser Lösung ist oben schon in Frage gestellt worden). Wer jedoch dieses Wörterbuch verwenden möchte, kann es vom FTP-Server des Universitätsrechenzentrums etwa nach Eingabe der URL

```
ftp://ftp2.uni-muenster.de/Win95/microsoft/
```

herunter laden (Im LAN entspricht er der PUBLIC-Platte.). Es ist die Datei `mssp2_ge.lex`, die man in das Verzeichnis

```
c:\Programme\Gemeinsame Dateien\Microsoft Shared\Proof
```

kopiert, falls `c:` der Laufwerksbuchstabe der Platte ist, auf der sich die betreffende Verzeichnisstruktur befindet. Wem dann die alte Schreibung von „daß“ nicht mehr gefällt, kann ja diese Schreibung (und weitere!) in einem Ausnahmewörterbuch zusammenstellen bzw. die alten und neuen Schreibungen für die Auto-Korrektur aufbereiten.

Es sei noch erwähnt, dass es Konverter-Programme gibt, z. B. das Programm ORTHOGRAF aus dem Bertelsmann-Verlag, mit denen man die alten Schreibungen in Word-Dateien in die neuen konvertieren kann.

StarWriter 4.0

Für StarOffice gibt es z. Zt. noch keine an die NDR angepasste Rechtschreibmodule, nach Aussage des Herstellers wird aber daran gearbeitet. Man empfiehlt vorerst, die neuen Schreibweisen in das aktuelle Wörterbuch aufzunehmen und die alten ins Ausnahmewörterbuch. Bei Verwendung der alten Schreibweise erhält man dann den Hinweis „Dieses Wort sollten Sie vermeiden“. Dieser Rat ist jedoch nur für die am häufigsten gebrauchten Neuschreibungen („daß“ – „dass“) praktikierbar. Für eine generelle Lösung empfehlen wir, dann schon lieber auf das neue Rechtschreibmodul zu warten!

Terminal Server an der WWU Windows – aber zuverlässig und ausfallsicher

H.-W. Kisker

Demnächst können Sie von Ihrem Arbeitsplatz aus über das Netz die Leistungsfähigkeit eines schnellen Windows-NT-Rechners testweise nutzen.

An der Universität Münster steht über das Zentrum für Informationsverarbeitung ab 2. November ein System von **Windows-NT-Servern** (Terminal Server Edition) zur allgemeinen Nutzung zur Verfügung. Angehörige der Universität können hier eine Reihe von Software-Produkten in den jeweils aktuellen Versionen von ihren Windows-Arbeitsplätzen aus nutzen:

- Adobe PhotoShop
- Corel WordPerfect Suite
- CorelDraw
- Microsoft Office Pro
- Microsoft FrontPage (einschließlich Server-Erweiterungen)

Die Programme laufen grundsätzlich auf dem Terminal Server und nicht auf dem Arbeitsplatz des Benutzers ab. Der Terminal Server ist ein NT-Server mit einer Multi-User-Erweiterung. Der Arbeitsplatz des Benutzers dient nur zur Anzeige der Programmfenster. Auf ihm muss ein Client-Programm installiert werden. Zur Zeit stehen Client-Programme nur für Windows-Arbeitsplätze zur Verfügung (WfW, Windows 95, Windows 98 und Windows NT). Erhältlich sind aber auch Client-Programme für viele andere Plattformen, z. B. Solaris, MacOS, Linux, AIX, IRIX; allerdings sind hiermit erhebliche Kosten verbunden.

Die Bereitstellung der Server ist als Evaluations-Projekt zu verstehen, durch das Erfahrungen gewonnen sowie Benutzerakzeptanz und Leistungsdaten ermittelt werden sollen. Als Zeitraum ist ein halbes Jahr, von November 1998 bis Mai 1999, vorgesehen. Für diese Zeit stellen die Firmen Adobe, Corel und Microsoft die obigen Software-Produkte kostenfrei zur Verfügung. Die Firma Microsoft stellt darüber hinaus noch alle Server- und Client-Lizenzen kostenfrei bereit. Bei einem Betrieb über diesen Zeitraum hinaus, müssen diese Produkte nachlizenzieren werden.

Alle weiteren Informationen (auch über Installation und Aufruf) erhalten Sie ab 2. November über das Internet an unserem neu aufgebauten Windows-Kiosk winKiosk.uni-muenster.de.

Dank für treue Dienste

W. Bosse

Wenn ein 25-jähriges Dienstjubiläum gefeiert wird, sind Worte des Dankes für treue Dienste üblich und auch angebracht. Wenn aber nun ein Jahr daran fehlt, wie steht es dann?

Unser bewährter Mitarbeiter Paul Kappelhoff ist zum 31.5.1998 nach 24-jähriger Tätigkeit im Operating in den Ruhestand getreten und hat eine spürbare Lücke hinterlassen. Nicht erst seit seinem Ausscheiden wissen wir, wie wertvoll er als engagierter und hilfsbereiter Kollege für uns und als kompetenter und freundlicher Partner für unsere Kunden war. Für die in all den Jahren geleistete Arbeit danken wir ihm deshalb an dieser Stelle ganz besonders.

Mitarbeiter im Maschinensaal eines Rechenzentrums werden im Tarifvertrag als „Angestellte in der Maschinenbedienung“ bezeichnet. Doch Herr Kappelhoff hat immer auch die Menschen bedient, nicht nur die Maschinen. Das zeichnete ihn aus. Darin war er ein Vorbild. Und dass er am liebsten noch viel länger aktiv geblieben wäre, was aber sein Gesundheitszustand leider nicht zuließ.

So gelten ihm für den neuen Lebensabschnitt unsere besten Wünsche, vor allem, dass er den verdienten Ruhestand bei guter Gesundheit genießen kann.

Nutzung des ADSM in der WWU

R. Mersch

Der ständig wachsende Datensicherungsbedarf mittels ADSM stellt hohe Anforderungen an das Management dieses Systems und macht die im Folgenden beschriebenen Regelungen erforderlich.

Eine 1995 durchgeführte Umfrage zur DV-Ausstattung in der WWU ergab u. a., dass auf vielen Rechnern keine Datensicherung durchgeführt wurde. Bei manchem Rechner ist das wohl auch nicht nötig, z. B. wenn es sich um einen Arbeitsplatzrechner mit einer Standardkonfiguration und ohne persönliche Daten handelt. In vielen Fällen sind aber benutzereigene Daten der Gefahr des unwiederbringlichen Verlustes ausgesetzt.

Mehr und mehr Benutzer begegnen dieser Gefahr durch den Einsatz des ADSM (*Adstar Distributed Storage Manager*) zur Sicherung, teilweise auch zur Archivierung, ihrer Daten. Mittlerweile haben 500 über die gesamte Universität verteilte ADSM-Clients über 32 Mio. Dateien mit einem Umfang von 2.3 TB im ADSM-Server deponiert. Dabei wird der ADSM auf unterschiedlichsten Plattformen eingesetzt (in Klammern jeweils die Anzahl registrierter Clients): AIX (38), BUTA (1), DEC UNIX (3), IRIX (1), LINUX (11), Mac (29), OS/2 (44), OSF/1 (1), PC/DOS (8), SCO (9), SINIXRM (1), Sun (50), ULTRIX (1), Win95 (66), WinNT (173), Windows (52).

Eine unmittelbare Konsequenz aus der wachsenden Anzahl von ADSM-Clients in der WWU ist, dass die Kosten für die Lizenzen, die der ADSM-Server für jeden eingetragenen ADSM-Client braucht, nicht mehr vom ZIV getragen werden können. Sie müssen daher den Fachbereichen bzw. den zuständigen IVVs in Rechnung gestellt werden. Z. Zt. betragen sie 32.80 DM (+ MWSt) pro ADSM-Client, es droht allerdings eine Preiserhöhung.

Im Folgenden sei beschrieben, was beim Einsatz des ADSM zu beachten ist.

Installation des ADSM-Clients

Die Version 2 der ADSM-Client-Software liegt auf unseren Unix-Rechnern im Verzeichnis `/dfs/a/urz/adsm/install`, die Version 3 im Verzeichnis `/dfs/a/urz/adsm/install/v3r1`. Dort gibt es Unterverzeichnisse für die verschiedenen an der WWU vorhandenen Plattformen. Wenn die gewünschte Plattform fehlt, sollte beim Autor nachgefragt werden, ob sie beschafft werden kann.

Zwar hat die Version 3 gegenüber der Version 2 erhebliche Vorzüge, leider aber auch hier und da noch einige Macken, so dass eine generelle Empfehlung zur Benutzung der Version 3 z. Zt. noch nicht gegeben werden kann. Sobald sich dies für eine bestimmte Plattform ändert, wird die Version 2 in den o. g. Verzeichnissen verschwinden bzw. durch die Version 3 ersetzt.

Neben den eigentlichen Installationspaketen finden sich in diesen Verzeichnissen zusätzliche Informationen:

- README-Dateien,
- evtl. BAT-Programme, die bei der Installation helfen,
- evtl. Muster-Konfigurationsdateien (`dsm.opt` bei den PC-Clients, `dsm.sys`, `inclexcl.def` und `dsm.opt` bei den Unix-Clients),
- evtl. weitere Hinweise vom ZIV in der Datei namens `Hinweise`.

All diese Dateien sollte man sich per FTP von einem unserer Unix-Rechner holen, die Installationspakete in jedem Fall im binären Modus, die BAT-Dateien in jedem Fall im ASCII-Modus. Das weitere Vorgehen wird in den READMEs beschrieben.

Anschließend sind die Konfigurationsdateien anzupassen. Falls keine Muster-Konfigurationsdateien vorhanden sind, sind auf jeden Fall die folgenden Einstellungen vorzunehmen (in der Datei `dsm.sys` auf Unix-Systemen, sonst in der Datei `dsm.opt`):

```

COMMmethod      TCPIP
TCPServeraddress  BACKUP.UNI-MUENSTER.DE

```

Die zweite Zeile gibt den Namen unseres ADSM-Servers an. Sinnvoll sind überdies die folgenden Eintragungen:

```

COMPression      ON
PASSWORDAccess   generate

```

Die erste Zeile spezifiziert, dass der ADSM-Client die zu übertragenden Daten komprimieren soll. Dies reduziert die Netzlast. Die zweite Zeile sorgt dafür, dass das ADSM-Passwort automatisch generiert wird. Nur bei Eröffnung der ersten ADSM-Sitzung wird es erfragt und dann in einer lokalen Datei verschlüsselt abgelegt, vorausgesetzt, der Aufrufer hat die nötigen Rechte (im Unix muss es der root-User sein).

Der Name, unter dem sich der ADSM-Client beim Server meldet, ist standardgemäß identisch mit dem Rechnernamen. Wenn Rechnername und Client-Name unterschiedlich sind, kann der Client-Name in der Konfigurationsdatei gesetzt werden:

```

NODEname         <Client-Name>

```

Ein Scheduler-gesteuertes (s. u.) oder mittels des Kommandos `dsmc incremental` angestoßenes Backup schreibt standardgemäß alle lokalen Dateibereiche ab. Wenn etwas anderes gewünscht ist, sollte man in der Datei `dsm.opt` (auch auf Unix-Rechnern diese Datei!) die folgende Eintragung vornehmen:

```

DOMain           <Dateibereich1> <Dateibereich2> ...
                 <DateibereichN>

```

Anmeldung (Registrierung) des ADSM-Clients

Der ADSM-Client muss im ADSM-Server eingetragen (registriert) werden. Die dazu erforderliche Lizenz im ADSM-Server muss der Nutzer vom ZIV (oder direkt von IBM) erwerben. Der genaue Bestellvorgang kann beim Autor erfragt werden.

Zur Registrierung des ADSM-Clients sind dem ADSM-Administrator formlos folgende Angaben zu machen:

Name des ADSM-Clients.

Er sollte identisch mit dem Namen des Rechners sein.

Anfangspasswort.

Nach der Registrierung sollte es umgehend geändert werden. (s. „Sicherheitsaspekte beim Einsatz von ADSM“)

Namen(n) und E-Mail-Adresse(n) der Kontaktperson(en).

Gelegentlich erhalten die Kontaktpersonen E-Mail, teils administrativen Inhalts, teils Hinweise auf Fehlersituationen. Sie sollten darauf reagieren können. Ferner sind die Kontaktpersonen, neben der Institutsleitung, die einzigen Personen, die sicherheitskritische Aktionen, wie etwa die Neusetzung des Passwortes, veranlassen können (s. „Sicherheitsaspekte beim Einsatz von ADSM“).

Fachbereich und Institut.

Umfang der zu sichernden Daten.

Hier geht es nur um eine grobe Einschätzung (in GB), die es erlaubt, eine Klassifizierung in Standard-Clients und sehr große Clients vorzunehmen.

Teilnahme am Scheduler-gesteuerten Backup erwünscht?

Die meisten PC-Benutzer ziehen es vor, das Backup nach eigenem Belieben von Hand anzustoßen. Bei Servern und Unix-Workstations, die nachts und am Wochenende durchlaufen, ist hingegen oft ein automatisches, nächtliches Backup durch den ADSM-Scheduler sinnvoll. Letzteres muss im ADSM-Server eingetragen werden. Das Scheduler-gesteuerte Backup wird durch einen Automatismus überwacht, der eine E-Mail an die Kontaktpersonen schickt, wenn es in der Nacht zuvor nicht gelaufen ist.

Betriebliche Regelungen

Durch den Einsatz des ADSM ergeben sich auch Verpflichtungen, die sich grundsätzlich aus dem Gebot, mit den Ressourcen verantwortlich umzugehen, ableiten. So kann man mit Hilfe der Include-Exclude-Liste in der Konfigurationsdatei dafür sorgen, dass nur die sicherungswürdigen Dateien abgeschrieben werden. Ferner sollte man Daten löschen, wenn sie nicht mehr gebraucht werden. Im Archiv-Bereich kann dies mit dem Kommando `delete archive` (oder über die grafische Oberfläche) geschehen.

Backups wird man in der Regel nicht löschen wollen, es sei denn, es handelt sich um Backups eines nicht mehr existierenden Dateibereichs (z. B. Platte, Partition oder Dateisystem). Der ADSM lässt die Backupkopien einer Datei nämlich nur verfallen, wenn im Zuge eines inkrementellen Backups (Teilsicherung) festgestellt wird, dass die Datei nicht mehr existiert. Gibt es den zugehörigen Dateibereich nicht mehr, kann auch kein inkrementelles Backup dieses Dateibereichs mehr durchgeführt werden und die Backupkopien bleiben prinzipiell für immer erhalten. Dies gilt sowohl bei Auflösung, als auch bei Umbenennung eines Dateibereichs; bei Umbenennung wird unter dem neuen Namen ein neues Backup erstellt, das alte bleibt erhalten.

Zum Löschen aller Backups und Archivdateien eines Dateibereichs bedient man sich des Kommandos `delete filespace` oder der grafischen Oberfläche. Falls der ADSM-Server diese Aktion nicht erlaubt (dies ist die Voreinstellung), sollte der ADSM-Administrator um Freigabe gebeten werden.

Das ZIV erwägt, künftig die Backups von Dateibereichen, die seit mehr als 100 Tagen nicht mehr abgeschrieben wurden, zu löschen. Feedback in diesem Punkt (wie grundsätzlich in allen Punkten) ist erwünscht; wem diese Regelung also zu rigoros erscheint, oder wer konkret Dateibereiche hat, deren Backups für längere Zeit eingefroren werden sollen, möge sich an den Autor wenden.

Wenn ein ADSM-Client nicht mehr benötigt wird, sollte dies dem ADSM-Administrator mitgeteilt werden, damit die Client-Lizenz anderweitig benutzt werden kann.

Der folgende Beitrag stellt sich der Frage, wie sicher die Daten im ADSM-Server sind.

Sicherheitsaspekte beim Einsatz von ADSM

R. Mersch

Beim Einsatz des ADSM ergibt sich eine Reihe unterschiedlicher Sicherheitsfragen. Sie betreffen zum einen den Schutz vor unberechtigtem Zugriff, zum anderen den Schutz vor Verlust der Daten.

Die Kontaktperson

Bei der Registrierung werden dem ADSM-Client eine oder mehrere Kontaktpersonen zugeordnet. Sie haben zwei Funktionen: Zum einen sind sie die Ansprechpartner des ADSM-Administrators in besonderen Situationen, oft Fehlersituationen der Art, dass ein Scheduler-gesteuertes Backup nicht gelaufen ist. Sie sollten dann in der Lage sein, die erforderlichen Schritte zu unternehmen.

Zum anderen sind die Kontaktpersonen, neben dem Institutsleiter, die einzigen Personen, die beim ADSM-Administrator sicherheitskritische Aktionen veranlassen können. Hierzu gehören: die Zuteilung eines neuen Passwortes (s. u.), das Löschen von Backups alter Dateibereiche, das Löschen des gesamten Clients, und schließlich die Eintragung einer neuen Kontaktperson.

Bei all diesen Aktionen besteht das Problem des sicheren Kommunikationskanals zwischen der Kontaktperson und dem ADSM-Administrator im ZIV. Der ADSM-Administrator muß sicherstellen können, dass die Anfrage wirklich von der angegebenen Kontaktperson kommt. Fernmündlich und, zumindest ohne weitere Vorkehrungen, per E-Mail ist dies nicht möglich. Der Standardweg ist, dass die Kontaktperson persönlich vorspricht und sich ausweist. Wenn die Kommunikation per E-Mail erfolgen soll, so muss diese mit PGP signiert werden. Der öffentliche Schlüssel der Kontaktperson ist

dazu dem ADSM-Administrator zu überbringen, z. B. per E-Mail. Dazu muss der Schlüssel entweder von einem anerkannten Zertifikatgeber zertifiziert sein (s. <http://www.uni-muenster.de/URZ/PGP/>), oder der Fingerprint muss persönlich samt Personalausweis vorgelegt werden. Zur Benutzung von PGP mit PINE gibt es einen Beitrag im WWW:

<http://www.uni-muenster.de/URZ/Hinweise/PGPmitPine.html>.

Das ADSM-Passwort

Eine zentrale Rolle beim Schutz vor unberechtigtem Zugriff spielt das Passwort des ADSM-Clients. Bei der Wahl und Handhabung des Passwortes ist größte Sorgfalt geboten, da jeder, der es kennt, Zugang zu allen Sicherungs- und Archiv-Kopien dieses ADSM-Clients erhalten kann.

Das Passwort kann bis zu 64 Zeichen lang sein und aus Buchstaben, Ziffern und den Zeichen + . _ - & bestehen. Groß- und Kleinschreibung werden nicht unterschieden.

Beim Start einer ADSM-Sitzung wird das Passwort nicht übertragen, so dass es nicht durch Abhören der Verbindung zwischen Client und Server ausgespäht werden kann. Da der ADSM-Server nicht dazu bewegt werden kann, seine (verschlüsselten) Passwörter herauszugeben, ist ein systematischer Angriff, wie etwa früher mit dem Crack-Programm im Unix-Bereich, nicht möglich. Wenn man ferner mittels der Setzung `PASSWORD-ACCESS GENERATE` in der Konfigurationsdatei dafür sorgt, dass das Passwort zu Beginn einer ADSM-Sitzung (außer der ersten) automatisch erzeugt wird, besteht die Gefahr, dass es beim Eintippen ausgespäht wird, auch nicht mehr.

Die Setzung `PASSWORDACCESS GENERATE` hat den weiteren Vorteil, dass man ein sehr langes Passwort wählen kann, da man es ja selten eintippen muss. Sollen außer dem System-Verwalter auch andere Benutzer den ADSM, z. B. zum Archivieren oder zum Restaurieren von Dateien, nutzen können, ist `PASSWORDACCESS GENERATE` ein Muss, da man ihnen das Passwort natürlich nicht mitteilen will.

Die Verwendung von `PASSWORDACCESS GENERATE` hat allerdings einen Nachteil: Das Passwort wird verschlüsselt in einer Datei auf dem ADSM-Client abgelegt, die, z. B. bei einer Neuinstallation, schon mal verloren gehen kann. Außerdem ist die Verschlüsselungsmethode abhängig von der Umgebung; bei Austausch beispielsweise des Rechners funktioniert das verschlüsselte Passwort nicht mehr. Wenn man es dann nicht mehr kennt – man hat es ja lange nicht mehr eingeben müssen – bleibt nur die Setzung eines neuen Passwortes durch den ADSM-Administrator (s. o.).

Verschlüsselung der Backup- und Archivdaten

... gibt es z. Zt. nicht. Obwohl seit langem gefordert, ist die ADSM-Client-Software nicht in der Lage, die zu übermittelnden Daten zu verschlüsseln. Wer also der Netzverbindung oder dem ADSM-Administrator nicht traut, hat nur die Möglichkeit, die Daten vor dem Erstellen der Backup- oder Archiv-Kopie selbst zu verschlüsseln.

Die Erweiterung der Client-Software um Verschlüsselungs-Funktionalität wurde allerdings auf dem ADSM-Workshop im September 1998 in Aussicht gestellt.

Verlust von Daten im ADSM-Server

Datenverluste im ADSM-Server selbst, etwa durch defekte Platten oder Magnetbandkassetten, sind nicht völlig auszuschließen, und in der Vergangenheit auch schon vorgekommen, obwohl bei der Wahl der Bandperipherie auf eine zuverlässige Technologie geachtet wurde.

Im Archiv-Bereich wird diesem Risiko dadurch Rechnung getragen, dass von der Archivkopie einer Datei eine zweite Kopie auf einem separaten Band erstellt wird. Zum vollständigen Verlust einer Archivdatei müssen also zwei Bänder gleichzeitig einen Defekt haben, und dies an der jeweils passenden (bzw. unpassenden) Stelle. Das Erstellen der zweiten Kopie geschieht nicht sofort, sondern in der folgenden Nacht. Wenn man also das Original nach dem Archivieren löschen will, sollte man dies erst am nächsten Tag tun, wenn man auf der sicheren Seite sein will.

Im Backup-Bereich ist die doppelte Speicherung der Daten zwar auch möglich, sie wird bei uns aber nicht betrieben. Dies hat natürlich Kostengründe, ist darüber hinaus aber auch Ergebnis der Überlegung, dass zwischen Originaldatei und Backupkopie eine symmetrische Beziehung herrscht: Ist das Original zerstört, kann es aus der Backupkopie wiederhergestellt werden, und umgekehrt genauso. Insofern ist man nicht schlechter dran, als im Archivbereich, wo die Originaldatei nach dem Archivieren oft bewusst gelöscht wird. (Diese Überlegung lässt Unterschiede in der Zuverlässigkeit der Datenträger außer Acht.)

In der Praxis sieht dies so aus, dass bei einem Verlust von Backupkopien die Kontaktpersonen der betroffenen ADSM-Clients vom ADSM-Administrator benachrichtigt werden. Ihnen werden die betroffenen Dateibereiche und, wenn es nicht zu viele sind, auch die betroffenen Dateien genannt. Wenn eine regelmäßige Sicherung dieser Dateibereiche über den Scheduler erfolgt, ist keine Aktion seitens der Kontaktpersonen erforderlich, andernfalls sollte umgehend ein inkrementelles Backup (Teilsicherung) angestoßen werden, das automatisch alles Erforderliche unternimmt.

Wem diese Maßnahmen nicht reichen, wer also beispielsweise für die Backups ausgewählter Dateien doppelte Speicherung benötigt, möge sich an den ADSM-Administrator wenden. Der ADSM verfügt über sehr feine Steuerungsmöglichkeiten, so dass Sonderbehandlungen bis hinunter auf Dateiebene definiert werden können. Wenn Sonderwünsche im Rahmen unserer Möglichkeiten liegen, werden wir ihnen gerne nachkommen.

Fingerabdrücke

R. Perske

Dieser Beitrag enthält die kryptografischen Prüfsummen der öffentlichen Schlüssel, die vom Zentrum für Informationsverarbeitung verwendet werden

Prüfsummen der PGP-Schlüssel der Mitarbeiter des ZIV

Diese PGP-Schlüssel befinden sich im World Wide Web unter der Adresse <http://www.uni-muenster.de/URZ/Mitarbeiter/urzring.asc>

Type	Bits/KeyID	Date	User ID
pub	2048/131B72ED	1998/08/18	Rainer Altvater <altvate@uni-muenster.de> Key fingerprint = FF 89 81 67 37 45 2B 1C 57 F5 BB DD 4A D5 04 60
pub	2048/EF750F1D	1997/10/14	Rainer Perske +49(251)83-31582 Certification Key Key fingerprint = 2F 38 6E F8 DC 2E D8 5E 5B 35 DB 49 8A E4 52 AF
pub	1536/E307C0B9	1997/10/14	Rainer Perske <perske@uni-muenster.de> Key fingerprint = F3 99 93 1F AC 06 0D 17 ED 93 35 19 F6 2D A3 22
pub	768/D782E369	1997/07/18	Klaus Reichel <reichel@uni-muenster.de> Key fingerprint = 6C 35 15 A9 E3 9E 83 4E 2E 95 4A F1 47 FC 7F 58
pub	1024/BD7873F5	1997/06/17	Jürgen Hölter <holters@uni-muenster.de> Key fingerprint = EA CB 47 AF 3A 79 96 B5 D3 46 C8 98 53 72 3F 2B
pub	2048/8D1993F9	1998/02/27	DaWIN-Team <dawin@uni-muenster.de> Key fingerprint = 4D 3F C7 49 F6 75 E1 AF 36 A3 F8 2C 04 86 F8 0F
pub	1024/525140B9	1997/09/01	JOIN Project Team <join@uni-muenster.de> Key fingerprint = 8C A9 DF 11 F5 21 89 DA 44 73 F1 FA 86 3A 1A 71
pub	1024/51F8EA05	1997/06/18	Mathias Grote <grote@uni-muenster.de> Key fingerprint = 0F 13 5B 2D 1D A5 9D 65 DF EA 41 6B CE E5 88 C2

pub 1024/44C661C5 1996/12/06 Stefan Ost <ost@uni-muenster.de>
 Key fingerprint = 6F DB 21 B4 67 EA C2 E0 E8 3D 78 28 7C 66 09 38

pub 1024/3EBBF595 1997/02/24 "Eberhard Sturm" <sturm@uni-muenster.de>
 Key fingerprint = 6C 9D B3 38 C0 8C 3C BB AF 55 2A 7B 6A C4 66 B6

pub 1024/3D37C6E1 1997/06/19 Dr. Klaus-Bolko Mertz <mertz@uni-muenster.de>
 Key fingerprint = CA 6F 8D 5C EB 67 EA 18 38 79 64 3D 64 4C 4A 8C

pub 1024/29A14DD1 1997/06/18 Reinhard Mersch <mersch@uni-muenster.de>
 Key fingerprint = F0 AF 2B F1 FE 55 7A 3A E6 0D C7 27 29 50 22 26

pub 1024/17817C39 1997/09/01 Manfred Sand <sand@uni-muenster.de>
 Key fingerprint = A1 2E 07 2D 59 81 6F 58 F9 B8 35 28 BF 9B 81 58

pub 1024/8A2097A5 1997/06/13 *** KEY REVOKED ***
 Rainer Perske <perske@uni-muenster.de>
 Key fingerprint = AA D7 57 F5 8F 14 A7 A5 C4 E2 CF 04 95 52 25 60

Prüfsummen der Zertifikate der zentralen WWW-Server

Herausgeber der Zertifikate ist:

Rainer Perske
 perske@uni-muenster.de
 Universitätsrechenzentrum
 Westfälische Wilhelms-Universität Münster
 Münster, Germany, DE

www.uni-muenster.de

Bezeichnung:

www.uni-muenster.de
 Universitätsrechenzentrum
 Westfälische Wilhelms-Universität Münster
 Münster, Germany, DE

Serial Number: 12 (0x0c)

Valid Not Before: Jun 26 13:42:45 1997 GMT

Not After : Dec 17 13:42:45 2002 GMT

Fingerprint=D0 : B9 : D4 : 0A : 47 : C3 : BE : 7D : A9 : 2E : DA : BB : BB : 56 : 1A : CB

user.uni-muenster.de

Bezeichnung:

user.uni-muenster.de
 Universitätsrechenzentrum
 Westfälische Wilhelms-Universität Münster
 Münster, Germany, DE

Serial Number: 16 (0x10)

Valid Not Before: Dec 3 15:48:16 1997 GMT

Not After : Dec 17 15:48:16 2002 GMT

Fingerprint=4F : D7 : 42 : 05 : 05 : AA : EE : 80 : FF : 35 : C7 : B4 : 53 : 09 : 6C : 1F

Prüfsummen der Zertifikate weiterer WWW-Server

Auf Wunsch zertifiziere ich auch weitere WWW-Server innerhalb der Universität. Dabei führe ich allerdings nur eine minimale Plausibilitätskontrolle durch und halte mich an keine vorgegebene Policy.

Wenn ein Server hier genannt wird, bedeutet dies nur, dass ich ein Zertifikat für den Server ausgestellt habe, jedoch nicht, dass der Server läuft oder für andere als interne

Zwecke des jeweiligen Instituts verwendet wird. Die Ausstellung des Zertifikats hat den einzigen Zweck, den Betreibern der WWW-Server verschlüsselte Datenübertragung zu ermöglichen, ohne dass sie gleich viel Geld an amerikanische Firmen überweisen müssen.

pcwi003.uni-muenster.de

Bezeichnung:

pcwi003.uni-muenster.de
Systemadministration WI
Westfälische Wilhelms-Universität
Münster, Germany, DE

Serial Number: 18 (0x12)

Valid Not Before: Mar 16 09:32:49 1998 GMT

Not After : Mar 16 09:32:49 1999 GMT

Fingerprint=31:BE:DB:3C:A7:9F:72:5E:91:EC:AC:90:1F:08:22:04

wildcat.uni-muenster.de

Bezeichnung:

wildcat.uni-muenster.de
Institut fuer Wirtschaftsinformatik
Westfaelische Wilhelms-Universitaet
Muenster, Germany, DE

Serial Number: 19 (0x13)

Valid Not Before: Sep 1 13:48:38 1998 GMT

Not After : Sep 1 13:48:38 1999 GMT

Fingerprint=78:CF:70:A7:81:69:AE:C4:7D:17:C5:BC:09:E1:42:6D

www-wi.uni-muenster.de

Bezeichnung:

www-wi.uni-muenster.de
Institut für Wirtschaftsinformatik
Universität Münster
Münster, Germany, DE

Serial Number: 20 (0x14)

Valid Not Before: Sep 15 12:33:41 1998 GMT

Not After : Sep 15 12:33:41 1999 GMT

Fingerprint=2E:6A:75:5B:A1:B5:79:2D:E3:13:E8:3B:2B:8B:C1:ED

Geplante Neubeschaffungen im Unix-Server-Bereich

St.Ost

Nachdem sowohl DFG und Finanzminister grünes Licht gegeben haben, können wir zum Jahresende wichtige Teile unserer Unix-Server-Infrastruktur ersetzen und verstärken.

Der erste Teil der geplanten Neu- und Ersatzbeschaffungen greift zum Jahresende. Es sollen die Server ersetzt und verstärkt werden, die entweder betrieblich besonders wichtig oder die besonders stark nachgefragt und am Ende ihrer Leistungsfähigkeit sind. Im Einzelnen:

- ein starker Mail/IMAP-Server zum Ersatz des Rechners mail
- zwei DCE-Security-Server
- zwei WWW-Server
- zwei WWW-Proxy-Server
- ein ausfallsicherer NetNews-Server
- 300 GB Raid-5 Plattenspeicher

Hinzu kommen jeweils ein Netz-Management-Server und ein Netz-Datenbank-Server.

Das Schwergewicht dieser Beschaffungsrunde liegt also in der Stärkung der Web-basierenden Dienstleistungen. Einwählen, E-Mail lesen und versenden, im Web surfen und News lesen: all dies soll durch die Beschaffung performanter werden. Ein guter Teil des zusätzlichen Plattenspeichers wird für Nutzerdaten verwendet werden.

Der zweite (und leider letzte) Beschaffungsteil greift im nächsten Jahr. Dann sollen insbesondere Server zum „Number Crunchen“ beschafft werden.

Aktuelles zu SPSS und SAS

S. Zörkendörfer

Zum Statistik-Paket SPSS gibt es neue Module. SPSS- und SAS-Nutzer unter Unix werden sich auf eine Migration vorbereiten müssen.

Am 1. Dezember beginnt ein neues Lizenzjahr der Hochschullandeslizenz NRW für **SPSS am PC**. Das ZIV (URZ) gibt Nutzungsberechtigungen für die Produkte dieses Vertrages an Einrichtungen der WWU sowie auch an Mitarbeiter und Studierende der WWU zur ausschließlich wissenschaftlichen Nutzung am häuslichen Arbeitsplatz zum Einzelpreis von 100 DM weiter. Für Studierende erfolgt die Verteilung durch den Broschürenverkauf des ZIV (URZ), der Bestellvorgang hierfür wird durch Aushänge insbesondere im Gebäude Einsteinstraße 60 beschrieben.

Die **deutsche Version 8 des SPSS für Windows** (Windows NT, Windows 95 und wohl auch Windows 98) wird die am häufigsten nachgefragte Version sein. Studierende der WWU können dieses Paket in dem von uns betreuten CIP-Pool (Einsteinstraße 60, Raum 107) nutzen. Sie enthält das Basisprodukt und die Optionen Professional Statistics, Advanced Statistics, Tables, Trends, Categories, Conjoint, Exact Tests, Missing Value Analysis. Zudem lassen sich die Produkte **CHAID** und **AMOS** unter dieser Lizenz nutzen; außerdem ist neu hinzugekommen die Windows-Version **SPSS Data Entry Builder** zur Erstellung von Eingabemasken und zur Dateneingabe – ich weise deshalb besonders auf dieses Produkt hin, weil die Folgeversionen eine bequeme Gestaltung einer Internet-Umfrage ermöglichen sollen. Die Lizenz umfasst **Axum5** (Technical Graphics and Data Analysis, allerdings ohne Mathcad). Ich gebe gerne Auskunft über die Bedingungen, Axum5 außerhalb der SPSS-Lizenz oder **Neuronal Connections** zu nutzen.

Im Rahmen eines Ferienkurses habe ich erfolgreich die wesentlichen Neuerungen der Version 8 erproben und vorführen können: Das Erstellen einer Eingabemaske unter Data Entry und die interaktive Grafik des Basisproduktes. Auch im laufendem Wintersemester wird im Vorlesungsangebot des Zentrums für Informationsverarbeitung (Universitätsrechenzentrum) eine Einführungsveranstaltung zum SPSS angeboten.

Außer der deutschen Version 8 werden wir auch die englische Version 8 sowie für Windows 3.x Version 6.13 und eine Mac-Version 6 verteilen können. Auf die Einholung eines Lizenzcodes für die veraltete MS-DOS-Version werde ich nun wohl endlich verzichten können.

Auf vielfache Nachfrage sei auch an dieser Stelle betont, dass in der Hochschullandeslizenz nicht alle Produkte der Firma SPSS eingeschlossen sind. Der Vertrag umfasst z. B. nicht Systat, SigmaPlot, DeltaGraph.

Nutzer des SPSS unter Unix (AIX und Solaris) mögen sich mit dem ZIV (URZ) in Verbindung setzen, um auf eine eventuelle Migration von dieser Plattform zum September 1999 vorbereitet zu sein.

Bezüglich des Statistical Analysis System **SAS** bleibt es nach derzeitigen Stand bei der Ankündigung, dass die Unix-Lizenz nicht über den Januar 1999 hin verlängert werden wird. Ich informiere gerne über den jeweilig aktuellen Stand der Verhandlungen und bin bei der Migration behilflich – wenn Sie mich rechtzeitig vor dem 31.1.1999 ansprechen. Die Windows-Lizenz (derzeit SAS 6.12 TS045) wird zum April in ein Verlängerungsjahr fortgesetzt werden, die Anmietung zusätzlicher Optionen ist nicht geplant.

Planeten, pv-wave und mpeg-movies

V. Conzelmann

Eine Wissenschaftlerin aus der Planetologie berichtet über eine Anwendung der vom Universitätsrechenzentrum bereitgestellten Visualisierungssoftware pv-wave.

Die Planeten unseres Sonnensystems sind für Planetenphysiker ein spannendes Betätigungsfeld. Am Institut für Planetologie gibt es eine Arbeitsgruppe Planetenphysik, die sich unter anderem mit der Thermodynamik unserer Nachbarplaneten beschäftigt.

Die erdähnlichen Planeten Merkur, Venus, Mars und auch der Erdmond können grob in einen Kern, der zum Großteil aus Eisen besteht, und eine äußere Gesteinsschale aufgeteilt werden. In Abbildung 1 ist der Aufbau von Mond, Mars und Merkur skizziert. Der schwarze innere Bereich bezeichnet den Eisenkern und die dunkelgraue äußere Schicht beschreibt den Gesteinsmantel. Hier zeigt sich deutlich, dass sich die Körper sowohl hinsichtlich ihrer Größe als auch in ihrem inneren Aufbau unterscheiden.

Ihre innere Struktur hat sich kurze Zeit nach der Entstehung unseres Sonnensystems vor etwa 4,5 Milliarden Jahren gebildet, dabei wanderte das dichtere Eisen zum Planetenzentrum und bildete den Kern.

Experimentelle Untersuchungen liefern uns eine Fülle von Daten, die den heutigen Zustand der Oberfläche des Planeten, der Zusammensetzung des Gesteins sowie die relevanten physikalischen Parameter beschreiben.

Wir untersuchen nun die thermische Entwicklungsgeschichte eines solchen Planeten von einem nur schlecht bekannten Anfangszustand vor 4,5 Milliarden Jahren bis heute. Ein spezielles Arbeitsgebiet ist die Konvektion des Planetenmantels. Das Mantelgestein befindet sich in einem festen Zustand. Trotzdem kann es sich über geologische Zeiträume (also gemessen in Millionen Jahren) bewegen. Aufgrund der Nichtlinearität der zu lösenden Gleichungen, die die Fluidbewegung beschreiben, können Modelle nicht von diesem relativ gut bekannten, heutigen Endzustand „rückwärts“ gerechnet werden. Es bleibt uns also nichts anderes übrig, als einen Anfangszustand zu definieren, mit dem man losrechnet und das Ziel ist natürlich, ein Modell zu finden, das in seinem Endzustand eine Vielzahl der Eigenschaften des heutigen Planeten beschreibt. Letztendlich helfen diese Modelle, den Anfangszustand und die Entwicklung unseres gesamten Sonnensystems zu verstehen.

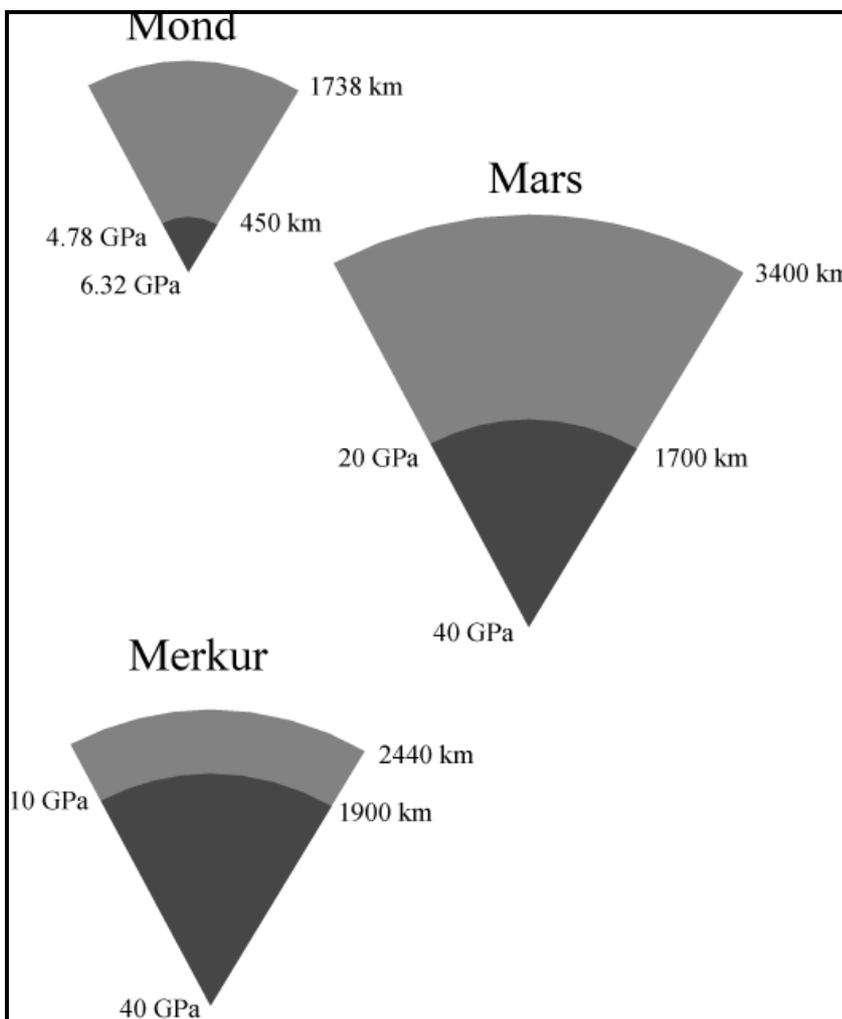


Abbildung 1:

Modelle zum inneren Aufbau von Mond, Mars und Merkur, wie sie in Konvektionsmodellen verwendet werden. Die relativen Größen der Abbildungen entsprechen den relativen Größen der Planeten. Ihre Zusammensetzung wurde nach geochemischen Modellen gewählt. Die Planeten können in einen eisenreichen Kern (schwarz) und einen silikatischen Mantel (dunkelgrau) aufgeteilt werden. Diese typische Schalenstruktur bildete sich unmittelbar im Anschluss an die frühe Zusammenballung der Planeten aus kleineren Gesteinsbrocken aus. Auf der linken Seite der Strukturmodelle sind die Drücke im Zentrum und an der Kern-Mantel Grenze in Gigapascal und rechts Planeten- und Kernradius in Kilometern aufgetragen.

Numerisch werden die fluiddynamischen Gleichungen mit einer Spektraltransformationsnäherung gelöst. Dabei werden auch die vom Rechenzentrum angebotenen IMSL-Routinen verwendet. An die grafische Darstellung der Ergebnisse der Konvektionsrechnungen werden hohe Ansprüche gestellt. Um den Bewegungsablauf des Mantelmaterials nachvollziehen zu können, müssen das Temperaturfeld und das Strömungspotential zu verschiedenen Zeitpunkten zur Verfügung stehen. In Abbildung 2 sind

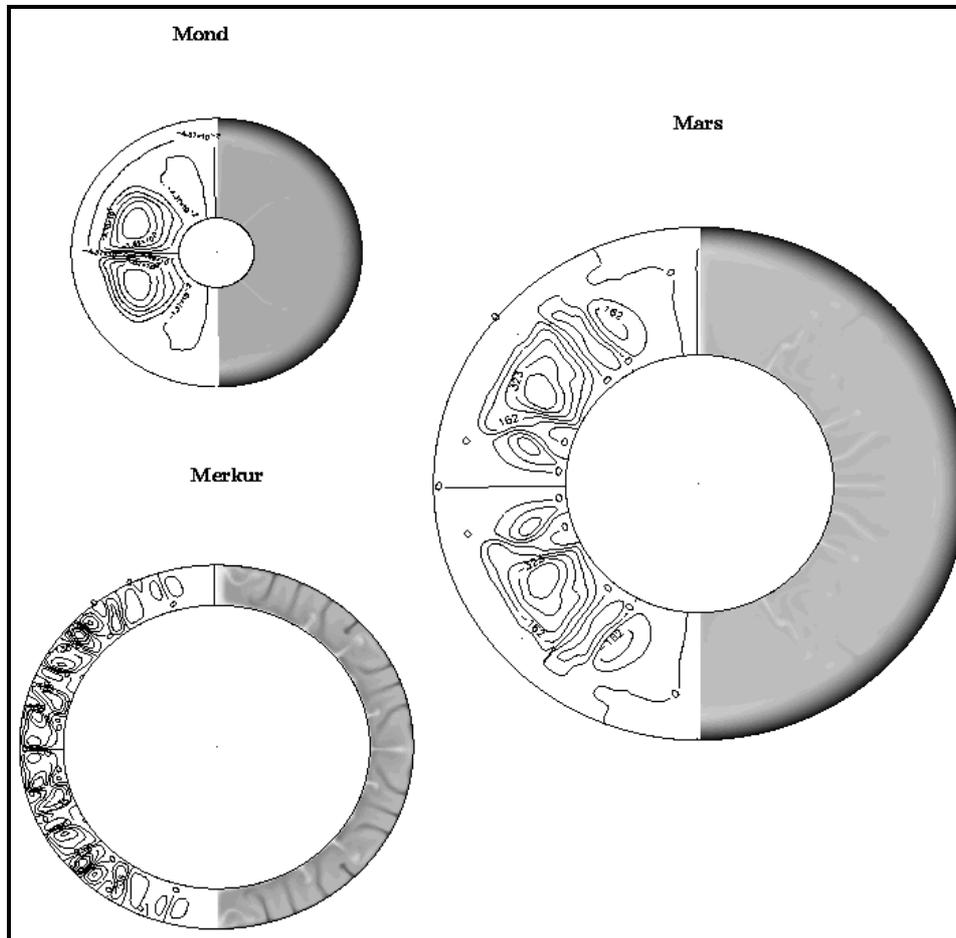


Abbildung 2:

Ergebnisbeispiele der Rechnungen für Mond, Mars und Merkur. Auch hier entsprechen die relativen Größen der Bilder den relativen Größen der Planeten. In den Abbildungen sind jeweils links das Strömungspotential und rechts die Temperaturverteilung dargestellt. Dabei sind hellgraue Bereiche am heißesten und dunkelgraue Bereiche am kältesten.

solche Bilder dargestellt. Es bietet sich an, diese Bilder zu einem Film zusammenzufassen, um die Evolution des Planeten am Bildschirm „live“ miterleben zu können.

Zur Erzeugung der Bilder wird das Grafikprogramm `pv-wave` benutzt, das vom Rechenzentrum für viele an unserer Uni verwendeten Plattformen angeboten wird. Der Vorteil dieses Programmpaketes liegt darin, daß man relativ komplexe Bilder in selbstgeschriebenen Programmen erstellen kann und eine Vielzahl von Routinen zur Verfügung steht. Diese vorgefertigten Routinen sind häufig nicht ganz fehlerfrei, jedoch erlaubt die Komplexität des Softwarepaketes in den meisten Fällen einen alternativen Weg, um das gewünschte Ergebnis zu erreichen. Die Programmierung ist natürlich oftmals zeitaufwendig, jedoch kann zumindest in diesem speziellen Fall kein anderes Grafikprogramm die Qualität des Endergebnisses übertreffen. Die Bil-

der in Abbildung 2 wurden mit zwei Routinen aus `pv-wave` erzeugt. Das Strömungspotential auf der linken Seite wurde mit `contour` dargestellt, das Temperaturfeld auf der rechten Seite musste aufgrund der komplexen Struktur mit `shade_surf_irr` erzeugt werden. Letztere Routine machte beim Ausdrucken in ein PostScript-File Probleme – merkwürdigerweise war die Auflösung auf dem Bildschirm besser als im PS-File. Zusätzlich war das in Graustufen dargestellte Temperaturfeld gegen die Begrenzungslinien verschoben und ein Teil der Datensätze konnte gar nicht dargestellt werden. Offensichtlich ein Programmierfehler im Grafikprogramm. Nach längerer Kommunikation mit dem technischen Support, den man unter `support@visual-numeric.de` erreichen kann, konnte das Problem umgangen werden. Eine Nachfrage beim support kann sich hier also durchaus lohnen.

Unter `pv-wave` werden auch Routinen angeboten, mit denen mehrere Bilder hintereinander dargestellt werden können. Diese stellten sich für diese Zwecke jedoch eher als unhandlich heraus, da alle Bilder in einem Verzeichnis vorgehalten werden müssen und

die CPU des Rechners stark beansprucht wird. Daher wurde beschlossen, die Bilder in mpeg-Filmen darzustellen. Dabei muss zwar ein Qualitätsverlust in Kauf genommen werden, die Filme sind jedoch viel anspruchsloser, was den Speicherplatz angeht und können zudem von anderen Benutzern, die nicht mit pv~wave arbeiten, angeschaut werden. Dafür werden zunächst alle Einzelbilder aus den Daten der Rechnungen mit pv~wave erzeugt. Dieser Vorgang wurde automatisiert, braucht allerdings Zeit und Plattenplatz. Ein einzelnes Bild im PostScript-Format ist 2 MB groß und in einem Film werden zwischen 400 und 2000 dieser Bilder verwendet. Die erzeugten Einzelbilder werden nun mit dem pbm~package ins YUV-Format umgewandelt, um dann mit dem Dienstprogramm mpeg daraus einen movie zu erstellen. Alle verwendeten Programme werden vom Rechenzentrum zur Verfügung gestellt. Mit eigenen Skript-Dateien werden diese Schritte weitgehend automatisiert. Wer sich diese Filme einmal anschauen möchte, findet sie unter <http://amadeo.uni-muenster.de/~conzelm>.

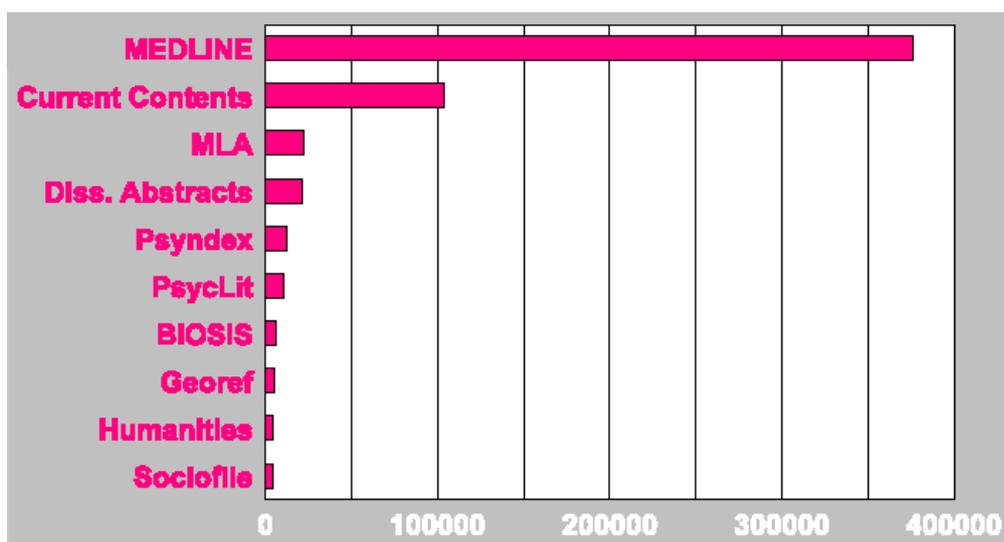
Nutzung der hochschulweit angebotenen Literaturdatenbanken

O. Obst, Zweigstelle Medizin der ULB

Datenbankrecherchen über das Uni-LAN werden immer beliebter. ULB und ZIV arbeiten bei deren Bereitstellung zusammen.

Neben 80 Inhouse-Datenbanken stellt die Universitäts- und Landesbibliothek (ULB) in Zusammenarbeit mit dem Zentrum für Informationsverarbeitung (Universitätsrechenzentrum) zehn Datenbanken im Hochschulnetz zur Verfügung. Durch eine Vielzahl von Clients für jedes Betriebssystem (Details finden Sie unter <http://medweb.uni-muenster.de/zbm/db/db3.htm>) kann jeder Angehörige der WWU komfortabel auf diese Datenbanken zugreifen – egal ob von der Bibliothek, vom Arbeitsplatz oder von zu Hause aus.

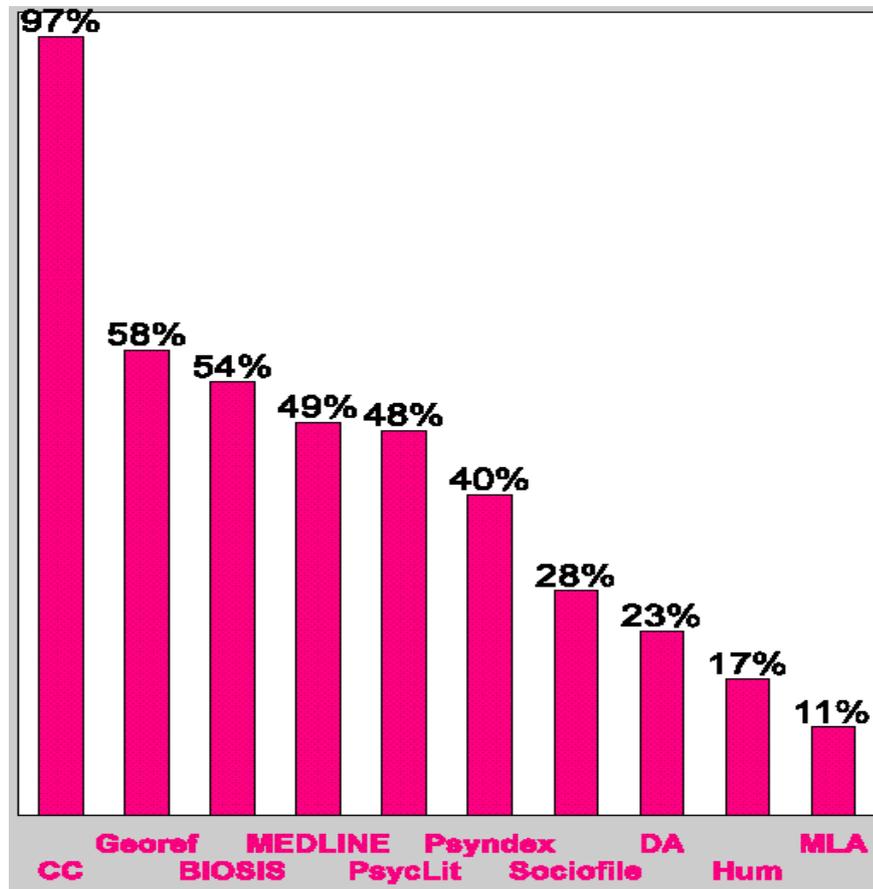
Wie die untenstehende Abbildung zeigt, wird dieser Service intensiv genutzt: Dabei ist die Literaturdatenbank MEDLINE mit knapp 376.000 Recherchen uneingeschränkter Spitzenreiter, gefolgt von *Current Contents* (CC). MEDLINE und CC alleine machen etwa 85% aller Suchsitzungen und mit 96.500 Stunden fast 89% der vor dem Suchbildschirm verbrachten Zeit aus. Insgesamt wurden 1997 in allen zehn Datenbanken 12.743.992 Zitate ausgedruckt bzw. kopiert. Dazu wurden von den Benutzern insgesamt 109.221 Stunden aufgewendet.



Benutzungshäufigkeiten der Datenbanken im Uni-LAN 1997

Die durchschnittliche Dauer jeder „Sitzung“ betrug 12 Minuten. Diese Statistik ist insofern bemerkenswert, wenn man sie mit den Zahlen für 1996 vergleicht: Die Zahl der ausgegebenen Zitate stieg um 130%, die Zahl der Suchen um fast 157% und die Gesamtdauer aller Suchen um über 180%. Dies bedeutet mehr als eine Verdoppelung innerhalb nur eines Jahres – ein Beweis für die stetig wachsende und überaus große Bedeutung elektronischer Medien bei der Informationssuche.

Die folgende Abbildung zeigt, wo die Datenbanken benutzt werden. *Current Contents* wird fast ausschließlich vom Arbeitsplatz aus benutzt, während die Datenbank der *Modern Language Association* (MLA) zu 88% in der Bibliothek durchsucht wird.



Zugriffe über das Uni-LAN in Prozent der Gesamtnutzung

RUM-Tutorial

Vertrauen ist gut, Kontrolle ist besser (1) Zugriffskontrolllisten im verteilten Dateisystem des DCE

B. Süselbeck

Mit einem Lenin-Zitat sei eine Folge von Artikeln über die Geheimnisse des DFS im Betriebssystem Unix eingeleitet.

Das *Distributed Computing Environment* (DCE) der *Open Software Foundation* (OSF) ist ein mächtiges System zur Realisierung verteilter Anwendungen in heterogenen Rechnerumgebungen. Es setzt auf vorhandene Betriebssysteme auf und stellt verschiedene Dienstleistungen zur Verfügung. Dies sind u. a. der *DCE Directory Service* zur Verwaltung von Rechnern und Benutzern, der *DCE Distributed Time Service* zur Synchronisation der beteiligten Rechner, der *DCE Security Service* zur Authentisierung und Autorisierung und – last but not least – der *DCE Distributed File Service* als verteiltes Dateisystem. Einen Überblick findet man in [1].

1 Un-Durchsichtig *Ein neues Dateisystem*

Der für den Anwender sicherlich wichtigste Bestandteil des DCE ist das *Distributed File System* (DFS). Es enthält insbesondere einen neuen Typus von Dateisystem, *Local File System* (LFS) genannt, der gegenüber den üblichen Unix-Dateisystemen eine ganze Reihe von Erweiterungen umfasst.

Der Endbenutzer merkt glücklicherweise bei der täglichen Arbeit überhaupt nicht, dass er sich in einem neuen Dateisystem befindet. LFS ist also zunächst für ihn transparent.

Ein wesentliches Merkmal von DCE gegenüber anderen verteilten Diensten ist die höhere Sicherheit. Ein solcher Anspruch lässt sich natürlich nur durch mehr Aufwand und strengere Kontrollen realisieren.

Bezogen auf das LFS bedeutet dieser Mehraufwand u. a. die Existenz von so genannten Zugriffskontrolllisten (*access control list*, ACL). Sie können jedem Objekt im LFS – Datei oder Verzeichnis – zugeordnet werden und beschreiben, welche Rechte Benutzer beim Zugriff auf Objekte haben. ACLs sind damit Erweiterungen der Zugriffsrechte unter Unix-Dateisystemen.

Da die ACLs ein Teil des DFS sind, der für den Anwender direkt von Bedeutung sein kann, soll dieser Aspekt der Sicherheit näher beleuchtet werden. Die folgenden Ausführungen sind daher für Benutzer gedacht, die – trotz aller Transparenz – mehr Durchblick erhalten wollen.

2 Dramatis Personae *Benutzer, Objekte, ACLs und Zellen*

ACLs sind Listen von Zugriffsprivilegien, die Objekten zugeordnet werden können. Eine ACL definiert Benutzerkategorien und weist ihnen Rechte (*permissions*) zu. Dadurch wird festgelegt, von wem und in welcher Weise auf das zugehörige Objekt zugegriffen werden darf.

Der Begriff *Objekt* ist im DCE recht weit gefasst. Er kann sich z. B. auch auf Benutzer und Rechner (im DCE-Jargon gemeinsam auch *Prinzipale* genannt) beziehen. Im folgenden werden jedoch nur die Zugriffskontrolllisten des DFS näher betrachtet. Sie gehören zu Dateien und Verzeichnissen. Die in diesem Kontext für ACLs gemachten

Aussagen lassen sich deshalb nicht immer auf andere Arten von DCE-Objekten übertragen.

Die DCE-Welt ist in sog. Zellen eingeteilt. Daher wird die Arbeit mit Zugriffskontrolllisten maßgeblich durch die Zugehörigkeit von Benutzern, Objekten und ACLs zu verschiedenen DCE-Zellen beeinflusst. Dabei kommt der Unterscheidung zwischen lokalen und fremden Zellen häufig eine entscheidende Bedeutung zu.

Bei der Klärung des Beziehungsgeflechts zwischen den oben vorgestellten Begriffen ist die Beantwortung der folgenden Fragen hilfreich:

- Welchem Benutzer gehört das Objekt?
- Welcher Gruppe gehört das Objekt?
- Zu welcher Zelle gehört ein Objekt?
- Zu welcher Zelle gehört eine ACL?
- Zu welcher Zelle gehört ein Benutzer?
- Zu welcher Zelle gehört eine Gruppe?
- Ist der Benutzer authentisiert?

Die Antworten auf diese Fragen legen zusammen mit diversen Regeln fest, welche Zugriffe von Benutzern auf Objekte erlaubt sind.

2.1 Eingesperrt – lokale, fremde und voreingestellte Zellen

Jedes Objekt im DFS gehört zu einer DCE-Zelle, die man auch *lokale Zelle* des Objekts nennt. Sie lässt sich aus dem vollständigen Namen entnehmen, z. B.:

```
/. . . /dce.uni-muenster.de/fs/u/s/suselbe
```

Er setzt sich aus der weltweiten Wurzel (/ . . .), der Kennzeichnung der lokalen Zelle

```
dce.uni-muenster.de
```

der Abkürzung (*fs*) für *filesystem* und dem individuellen Teil (hier *u/s/suselbe*) zusammen. Die Bezeichnung „weltweit“ ist übrigens wörtlich zu nehmen. Die Dateisysteme der einzelnen Zellen lassen sich zu einem globalen Baum zusammensetzen.

Das Verzeichnis mit dem Basisnamen *suselbe* gehört also zur Zelle

```
dce.uni-muenster.de
```

Alle anderen DCE-Zellen nennt man in Bezug auf dieses Objekt *fremd*.

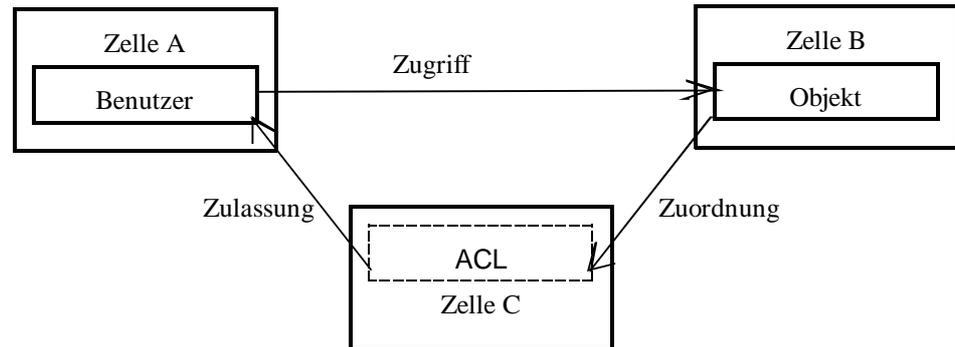
Auch jeder Benutzer gehört zu einer Zelle, wie sich an der Namensgebung unschwer erkennen lässt:

```
/. . . /dce.uni-muenster.de/suselbe
```

Dadurch werden insbesondere auch die Benutzerkennungen weltweit eindeutig. Ein Prinzipal, der sich gegenüber dem Sicherheitsdienst von DCE authentisiert hat, wird für eine gewisse Zeit (der Lebensdauer des entsprechenden Tickets) als vertrauenswürdig betrachtet. Alle anderen Benutzer gelten als nicht authentisiert.

Eine ACL hat keinen eigenen Namen. Sie wird über das Objekt, dem sie zugeordnet ist, erreicht und ist in dessen lokaler Zelle abgelegt. Die ACL besitzt aber noch die so genannte *voreingestellte Zelle* (*Default Cell*), die nicht mit der Zelle übereinstimmen muss, zu der das Objekt gehört! Für die Interpretation der Einträge in einer ACL ist die *Default Cell* entscheidend. Immer wenn sie von der lokalen Zelle des zugeordneten Objekts oder des zugreifenden Benutzers abweicht, sind Besonderheiten zu beachten.

Zwischen Benutzern, Objekten und Zugriffskontrolllisten besteht eine Art Dreiecksverhältnis:



Ein Benutzer aus Zelle A versucht auf ein Objekt in Zelle B zuzugreifen, das durch eine ACL mit der voreingestellten Zelle C geschützt ist (durch Strichelung angedeutet). Die drei Zellen können dabei verschieden sein, müssen es jedoch nicht.

Ein Beispiel für ein Objekt, das zu einer Zelle gehört, aber eine ACL besitzt, die eine andere Zelle voreingestellt hat, ergibt sich aus folgender Situation:

Die Organisation mit der Zelle

`dce.uni-muenster.de`

beauftragt eine Firma, im Dateisystem dieser Zelle ein Softwareprodukt zu installieren und zu warten, z. B. im Verzeichnis

`/.../dce/uni-muenster.de/fs/software.`

Die Firma hat die Zelle

`dce.software.com`

Dann könnte das oben genannte Verzeichnis bzgl. der Interpretation seiner ACL weiterhin zur Zelle

`dce.software.com`

gehören, obwohl es sich in der Zelle

`dce.uni-muenster.de`

befindet. Außerdem wäre es möglich, dass ein Benutzer aus einer dritten Zelle, z. B.

`dce.uni-stuttgart.de`

auf diese Software zugreift.

2.2 Klassengesellschaft – Benutzerkategorien in ACLs

Eine ACL besteht aus Einträgen, die Kategorien von Benutzern definieren und diesen Kategorien bestimmte Rechte zuordnen. Die Syntax dieser Einträge sieht folgendermaßen aus:

`{ type [key] permissions }`

Die ersten beiden Felder legen die Kategorie fest, das dritte Feld führt die entsprechenden Zugriffsrechte auf.

Die möglichen Kategorien sind in der folgenden Tabelle zu sehen²:

² Es gibt noch weitere Kategorien, die mit dem so genannten Delegationsmodell des DFS zusammenhängen (siehe [2]), das aber hier nicht weiter behandelt wird.

Typ	Schlüssel	Benutzer	Zelle
user_obj		Eigentümer	Default Cell
user	<i>username</i>	<i>username</i>	Default Cell
foreign_user	<i>cellname/username</i>	<i>username</i>	<i>cellname</i>
group_obj		in Eigentümergruppe	Default Cell
group	<i>groupname</i>	in <i>groupname</i>	Default Cell
foreign_group	<i>cellname/groupname</i>	in <i>groupname</i>	<i>cellname</i>
other_obj		beliebig	Default Cell
foreign_other	<i>cellname</i>	beliebig	<i>cellname</i>
any_other		beliebig	beliebig
mask_obj		Maske für andere Typen	

Der Typ definiert Benutzer oder Gruppen von Benutzern in der lokalen oder in fremden Zellen. Je nach Bedeutung muss in einigen Fällen als Schlüssel noch ein konkreter Benutzer-, Gruppen- oder Zellname angegeben werden. Die beiden rechten Spalten erklären, welche Benutzer in welcher Zelle durch die entsprechende Typ/Schlüssel-Kombination definiert werden. Man beachte dabei, dass ein Benutzer oder eine Gruppe erst durch die (implizite bzw. explizite) Angabe der Zelle vollständig qualifiziert ist.

So werden beispielsweise durch die ACL

```
{user_obj permissions}
```

für den Eigentümer des Objekts die in *permissions* festgelegten Rechte vergeben (dieser Typ benötigt keinen Schlüssel).

Die Typ/Schlüssel-Kombination in der ACL

```
{user suselbe permissions}
```

setzt Rechte für den Benutzer *suselbe*.

Die Einträge *user_obj*, *group_obj*, *other_obj* sowie *user* und *group* werden in der **Default Cell** der ACL interpretiert und nicht in der lokalen Zelle des zugehörigen Objekts, d. h. möglicherweise in einer für das Objekt selbst fremden Zelle.

Für die Kategorien in einer ACL gelten folgende Nebenbedingungen:

- Die Einträge *user_obj*, *group_obj* und *other_obj* müssen vorhanden sein.
- Wenn außer diesen drei Einträgen noch andere Kategorien vorkommen, dann muss auch ein *mask_obj*-Eintrag vorhanden sein.
- Alle anderen Einträge sind optional.

Die in *mask_obj* definierte Maske stellt eine Obergrenze der Rechte für alle Kategorien außer *user_obj* und *other_obj* dar, d. h. nur Rechte, die sowohl in der Kategorie als auch in der Maske gesetzt sind, werden vergeben.

2.3 Was gefällt, ist noch nicht erlaubt – Zugriffsrechte im LFS

Auch die Zugriffsrechte, die mit Hilfe einer ACL vergeben werden, haben gegenüber Unix gewisse Erweiterungen erfahren. Neben den bekannten Rechten *r*, *w*, *x* kommen noch die Rechte *c*, *i*, *d* hinzu.

Das Recht *c* für *control* besteht darin, die Zugriffsrechte für ein Objekt ändern zu dürfen. Unter Unix vermag dies nur der Eigentümer des Objekts bzw. der Superuser. Im DCE kann dieses Recht auch anderen Benutzerkategorien gewährt werden. Die beiden weiteren zusätzlichen Rechte haben nur für Verzeichnisse eine Bedeutung. Sie stehen für *insert* und *delete*, also für das Anlegen bzw. Entfernen von Objekten.

Im Folgenden sollen einige Aktionen und die dazu erforderlichen Rechte aufgelistet werden. Dazu sollte man sich noch einmal in Erinnerung rufen, dass bei der Bestimmung, ob ein gewünschter Zugriff auf ein Objekt erlaubt oder zurückgewiesen wird, die Zugriffsrechte aller Objekte im vollständigen Namen des Objekts geprüft werden, d. h. die Zugriffsrechte aller im absoluten Pfad stehenden Verzeichnisse und die Zugriffsrechte des Objekts selbst (Datei oder Verzeichnis).

Deshalb muss grundsätzlich bei beliebigen Aktionen in allen Verzeichnissen, die zu dem Objekt führen, das *x*-Recht gesetzt sein. Für das Objekt selbst und das unmittelbare Elternverzeichnis sind folgende Rechte erforderlich:

Aktion	Rechte für das Elternverzeichnis	Rechte für das Objekt
Datei lesen	<i>x</i>	<i>r</i>
Datei schreiben	<i>x</i>	<i>w</i>
Programmdatei ausführen	<i>x</i>	<i>x</i>
Shell-Skript ausführen	<i>x</i>	<i>rx</i>
In ein Verzeichnis wechseln	<i>x</i>	<i>x</i>
Verzeichnis auflisten	<i>x</i>	<i>r</i>
Informationen über Objekt anzeigen	<i>rx</i>	–
Objekt erzeugen	<i>wxi</i>	–
Objekt löschen	<i>wxd</i>	–
Objekt umbenennen	<i>wxd</i> (Quellverzeichnis), <i>wxi</i> (Zielverzeichnis)	– oder <i>w</i> ³
ACL eines Objekts anzeigen	<i>x</i>	–
ACL eines Objekts ändern	<i>x</i>	<i>c</i>

Eine ACL der Form

```
{user suselbe crwx}
```

gibt beispielsweise dem Benutzer *suselbe* die Rechte *crwx*.

Bei den Zugriffsrechten gilt die Nebenbedingung, dass das *c*-Recht im *user_obj*-Eintrag immer vorhanden sein muss.

³ Wenn ein Verzeichnis umbenannt wird (Kommando *mv*), dann muss in ihm selbst der Verweis auf das Elternverzeichnis geändert werden, falls sich Quell- und Zielverzeichnis unterscheiden. In diesem Fall ist auch für das Objekt selbst das *w*-Recht erforderlich.

2.4 Alte Privilegien – Rechte unter Unix

Im Unix-Dateisystem besitzt jede Datei die so genannten *mode bits*, die neben dem Typ der Datei auch die Zugriffsrechte für die Unix-Kategorien `user`, `group` und `other` festlegen. Sie werden bekanntlich, neben anderen Informationen, in der Ausgabe von `ls -l` angezeigt. Eine Änderung erfolgt mit Hilfe des Kommandos `chmod`.

Auch im DFS existieren die *mode bits* weiterhin. Sie sind im Gegensatz zu ACLs immer vorhanden. Existieren beide, so müssen sie natürlich synchronisiert werden, d. h. jede Änderung an einer der beiden Stellen wird automatisch an der anderen Stelle übernommen und zwar gemäß folgender Aufstellung:

Unix <i>mode bits</i>	ACL-Eintrag	ACL-Rechte
user	user_obj	r w x
other	other_obj	r w x
group	mask_obj	r w x
	falls mask_obj-Eintrag vorhanden	
	group_obj	r w x
	falls mask_obj-Eintrag nicht vorhanden	

Jede Änderung der ACLs, z. B. mit Hilfe von `dcecp` (siehe Seite 28) wird auf die Unix *mode bits* übertragen. Werden diese mit `chmod` geändert, so erfolgt ebenfalls eine Anpassung der zugehörigen ACL.

3 Greifen Sie zu!

Vergabe der Zugriffsrechte

Wenn ein Benutzer auf ein Objekt unter DCE zugreift, dann werden mit Hilfe der zugehörigen ACL die passenden Zugriffsrechte ermittelt. Damit steht fest, ob die gewünschte Aktion erlaubt ist oder nicht.

Dazu muss der Benutzer genau einer der in der ACL aufgelisteten Kategorien zugeteilt werden. Dies ist jedoch nicht ganz trivial, da ein Benutzer zunächst durchaus zu mehreren Einträgen passen kann.

Bei der Ermittlung der Zugriffsrechte wird folgender Weg eingeschlagen:

1. Es wird festgestellt, ob der Benutzer authentisiert ist.

Ist dies nicht der Fall, erhält er die Kennungen `nobody` bzw. `nogroup` und wird wie ein authentisierter Benutzer aus einer nicht existierenden Zelle betrachtet. Durch diesen Kunstgriff bildet der nichtauthentisierte Benutzer für das weitere Vorgehen keine Ausnahme mehr.

2. Die Einträge in der ACL werden in einer bestimmten Reihenfolge durchsucht, und zwar von mehr zu weniger spezifizierten.

Beim ersten passenden Eintrag endet die Suche.

Die Reihenfolge ergibt sich aus folgender Liste:

- Ist der Benutzer Eigentümer des Objekts, erhält er die Zugriffsrechte aus dem `user_obj`-Eintrag.
- Existiert ein passender `user`- oder (im ausschließenden Sinn!) `foreign_user`-Eintrag, so werden die zugehörigen Rechte durch die Rechte im `mask_obj`-Eintrag gefiltert und an den Benutzer gegeben.
- Ist der Benutzer Mitglied in der Gruppe aus dem `group_obj`-Eintrag oder in einer anderen Gruppe aus den `group`- bzw. `foreign_group`-Einträgen, so werden die zugehörigen Rechte akkumuliert, anschließend durch den `mask_obj`-Eintrag gefiltert und an den Benutzer gegeben.
- Der Benutzer ist in der voreingestellten Zelle definiert. Dann erhält er die Rechte aus dem `other_obj`-Eintrag. Es erfolgt keine Filterung durch `mask_obj`.
- Der Benutzer stammt aus einer fremden Zelle mit einem zugehörigen `foreign_other`-Eintrag. Dann werden die zugehörigen Rechte durch den `mask_obj`-Eintrag gefiltert und an den Benutzer gegeben.
- Der Benutzer stammt aus einer beliebigen Zelle. Nach Filterung durch die Maske erhält er die Rechte aus dem `any_other`-Eintrag, wenn er existiert.
- Der Benutzer erhält keine Rechte.

Gemäß dem oben vorgestellten Algorithmus kann ein nicht authentisierter Benutzer höchstens die Rechte aus dem `any_other`-Eintrag der ACL des Objekts erhalten, da er aus einer unbekanntenen Zelle stammt, d. h. weder aus der voreingestellten Zelle noch sonstigen fremden Zellen.

Eine weitere Konsequenz aus diesem Vorgehen ist, dass ein Benutzer über einen Gruppeneintrag nicht mehr Rechte erhalten kann, als über einen Benutzereintrag. Ist der Benutzer Eigentümer der Datei und gibt es für ihn zusätzlich einen Benutzer- oder Fremdbenutzer-Eintrag, so stammen die zugeteilten Rechte nur aus dem Eigentümereintrag. Bei der Mitgliedschaft in mehreren Gruppen werden die Rechte jedoch akkumuliert.

LFS-Dateisysteme lassen sich auf der entsprechenden Server-Maschine auch lokal bereitstellen. Dann hat man zwei Möglichkeiten auf Dateien in diesem System zuzugreifen:

- über den lokalen Pfadnamen
- über den Pfadnamen im DFS

In beiden Fällen wird beim Zugriff nach obigem Algorithmus verfahren. Sind allerdings die Identitäten im Unix und DCE unterschiedlich, so gilt im ersten Fall die Unix-Kennung und im zweiten Fall die DCE-Kennung.

Meldet man sich beispielsweise als `root` auf einer Maschine an, identifiziert sich später aber bei DCE mit seiner persönlichen DCE-Kennung, dann hat man beim Zugriff auf ein Objekt über den lokalen Pfadnamen `root`-Rechte. Beim Zugriff nach DFS-Konventionen erhält man die Rechte gemäß der DCE-Kennung.

Greift man als `root` nach DFS-Konventionen zu, so hat man die Kennung

```
/. . ./cellname/hosts/hostname/self
```

Um also Prozesse, die unter `root`-Kennung laufen, den Zugriff auf Dateisysteme nach DFS-Konventionen zu gewähren, muss die entsprechende `self`-Kennung geeignete Rechte haben.

4 Do it yourself

Bearbeiten von ACLs

Für die Verwaltung der meisten DCE-Komponenten gibt es das Ober-Kommando `dcecp` (*dce control program*). Nach dem Aufruf gelangt man in einen interaktiven Modus:

```
dcecp>
```

Zur Bearbeitung von ACLs dient dort das Unter-Kommando `acl`. Es realisiert für ACLs ähnliche Funktionen wie die Kommandos `ls` und `chmod` für Unix-Rechte. Die durchzuführende Aktion wird zusammen mit dem Namen des zu bearbeitenden DFS-Objekts als Argument übergeben, evtl. gefolgt von weiteren Optionen.

Die einfachste Anwendung ist die Auflisten der ACL eines Objekts:

```
dcecp> acl show .
{user_obj rwxcid}
{group_obj -----}
{other_obj -----}
```

Angezeigt werden die vorhandenen Einträge der ACL des aktuellen Verzeichnisses. In diesem Beispiel sind nur die minimal notwendigen Kategorien vorhanden.

Die voreingestellte Zelle erfährt man folgendermaßen:

```
dcecp> acl show . -cell
/.../dce.uni-muenster.de
```

Mit Hilfe der Aktion `modify` lassen sich neue Einträge erzeugen oder vorhandene Einträge modifizieren bzw. löschen:

```
dcecp> acl modify . -change {user_obj rwxid}
Error: not a valid DFS acl
```

Hier wird versucht, über die Option `-change` den Eintrag für `user_obj` zu ändern. Dieses Beispiel zeigt allerdings, dass das Löschen des Kontrollrechts `c` beim Eigentümer nicht möglich ist.

Rechte für einen einzelnen Benutzer lassen sich folgendermaßen hinzufügen:

```
dcecp> acl modify . -add {user licmgr rx}
dcecp> acl show .
{mask_obj r-x---}
{user_obj rwxcid}
{user licmgr r-x---}
{group_obj -----}
{other_obj -----}
```

Hier wird das Lese- und Ausführungsrecht für den Benutzer `licmgr` hinzugefügt. Wenn ein `user`-Eintrag vorhanden ist, muss wegen oben erläuterten Nebenbedingungen auch ein `mask_obj`-Eintrag vorhanden sein. Er wird, falls erforderlich aber noch nicht vorhanden, automatisch erzeugt und enthält die gleichen Rechte wie der neue Eintrag.

Im Folgenden soll der Benutzer `swm` die Rechte `rwx` erhalten:

```
dcecp> acl modify . -add {user swm rx}
dcecp> acl show .
{mask_obj rwx---}
{user_obj rwxcid}
{user licmgr r-x---}
{user swm rwx---}
{group_obj -----}
{other_obj -----}
```

Es zeigt sich, dass die Maske bei Eintrag eines neuen Feldes, das durch sie zu filtern ist, automatisch angepasst wird. Dies ist allerdings nicht immer der Fall, wie man nach Einschränkung der Rechte für die Maske erkennt:

```
dcecp> acl modify . -change {mask_obj rx}
dcecp> acl show .
{mask_obj r-x---}
{user_obj rwxcid}
{user licmgr r-x---}
{user swm rwx--- effective r-x---}
{group_obj -----}
{other_obj -----}
```

Hat ein Eintrag, der von der Maske gefiltert wird, mehr Rechte als die Maske, so zeigt der Kommentar `effective` die wirklichen Rechte an.

```
dcecp> acl modify . -add {group bin rwx}
Error: Unintended permissions not granted.
```

Würde in diesem Beispiel die Maske wieder automatisch die Rechte `rwx` zugewiesen bekommen, erhielte der Benutzer `swm` mehr Rechte als er momentan effektiv hat. Dies ist nicht erlaubt und führt deshalb zu einem Fehler. In diesem Fall muss eine zusätzliche Option angegeben werden, die genau spezifiziert, was mit der Maske geschehen soll:

```
dcecp> acl modify . -add {group u0rz rwx} -mask nocalc
dcecp> acl show .
{mask_obj r-x---}
{user_obj rwxcid}
{user licmgr r-x---}
{user swm rwx--- effective r-x---}
{group_obj -----}
{group u0rz rwx--- effective r-x---}
{other_obj -----}
```

Hier wird die Maske nicht (`-mask nocalc`) verändert. Dies hat zur Folge, dass die neu eingerichtete Gruppe auch nur die effektiven Rechte `rx` besitzt. Eine Neuberechnung der Maske kann durch die Option `-mask calc` erzwungen werden:

```
dcecp> acl modify . -add {group u0math rwx} -mask calc
dcecp> acl show .
{mask_obj rwx---}
{user_obj rwxcid}
{user licmgr r-x---}
{user swm rwx---}
{group_obj -----}
{group u0rz rwx---}
{group u0math rwx---}
{other_obj -----}
```

Damit erhält die neue Gruppe die im Kommando aufgeführten Rechte, aber auch die schon bestehenden Einträge für die Gruppe `u0rz` und den Benutzer `swm`.

Mit Hilfe der Option `-remove` lassen sich Einträge löschen:

```
dcecp> acl modify . -remove mask_obj
Error: not a valid DFS acl
```

Die Maske darf allerdings erst dann gelöscht werden, wenn alle durch sie gefilterten Einträge (außer `group_obj`) verschwunden sind:

```
dcecp> acl modify . -remove {{user licmgr} {user swm}}
dcecp> acl modify . -remove {{group u0rz} {group u0math}}
dcecp> acl modify . -remove mask_obj
dcecp> acl show .
{user_obj rwxcid}
{group_obj -----}
{other_obj -----}
```

Damit befindet sich die ACL wieder im ursprünglichen Zustand.

Ruft man das Ober-Kommando `dcecp` mit der Option `-c` auf, dann lassen sich die Unter-Kommandos auch nicht interaktiv ausführen:

```
$ dcecp -c acl help
check          Returns ACL permissions of invoker.
delete         Deletes all ACL entries except user_obj entry
               if it exists.
modify         Adds, removes, or changes ACL entries and at-
               tributes.
permissions    Returns permissions associated with an object.
replace        Replaces entire ACL with new ACL entries and
               attributes.
show           Returns ACL entries or attributes on an ob-
               ject.
help           Prints a summary of command-line options.
operations     Returns the valid operations for command.
```

Die Ausgabe des Hilfetextes zeigt weitere Möglichkeiten der ACL-Bearbeitung.

Wenn man sich die ACL eines Objekts anzeigen lassen möchte, benötigt man das `x`-Recht für alle Verzeichnisse, die zum Objekt führen. Will man Änderungen an der ACL durchführen, ist außerdem das `c`-Recht für das Objekt selbst erforderlich.

Die voreingestellte Zelle einer Object ACL kann mit Hilfe der Option `-cell` der Aktion `modify` geändert werden, aber nur vom einem Administrator der Zelle, zu der das Objekt gehört:

```
$ mkdir testdir
$ dcecp
dcecp> acl modify testdir -add {any_other c}
dcecp> acl show testdir
{mask_obj ---c--}
{user_obj rwxcid}
{group_obj -----}
{other_obj -----}
{any_other ---c--}
dcecp> acl show testdir -cell
/.../dce.uni-muenster.de
dcecp> acl modify testdir -cell /.../dce.uni-stuttgart.de
dcecp> acl show testdir -cell
/.../dce.uni-stuttgart.de
dcecp> exit
$ cd testdir
ksh: testdir: permission denied
```

Obwohl der Benutzer `suselbe` aus der Sicht von Unix Eigentümer des Verzeichnisses ist und eigentlich entsprechende Rechte hat, kann er nicht in das Verzeichnis wechseln. Das liegt natürlich daran, dass seine Privilegien nun anhand der Zelle `/.../dce.uni-stuttgart.de` festgestellt werden. Da der `user_obj`-Eintrag immer lokal zur voreingestellten Zelle der ACL geprüft wird, fällt der Eigentümer nun nicht in diese Kategorie.

Hier ist er lediglich in der Kategorie `any_other` zu finden

```
$ dcecp -c acl check testdir
---c--
```

wie man mit Hilfe der Aktion `check` leicht feststellen kann.

Da diese Kategorie hier das Kontrollrecht hat (in der Praxis wäre das sicher unüblich), kann sich der Anwender nun in der Kategorie hochsetzen:

```
dcecp> acl modify testdir -add \
> {foreign_user ../../dce.uni-muenster.de/suselbe rwxcdi}
dcecp> acl show testdir
{mask_obj rwxcid}
{user_obj rwxcid}
{foreign_user ../../dce.uni-muenster.de/suselbe rwxcid}
{group_obj -----}
{other_obj -----}
{any_other ---c--}
dcecp> acl check testdir
rwxcid
dcecp> exit
$ cd testdir
```

Das Ändern der voreingestellten Zelle einer ACL ist immer etwas problematisch, insbesondere weil sich dabei u. a. die Interpretation der `user`- und `foreign_user`-Einträge vertauschen müsste. So lässt sich im letzten Beispiel die voreingestellte Zelle nicht ohne weiteres rückgängig machen:

```
$ dcecp
dcecp> acl modify testdir -cell ../../dce.uni-muenster.de
Error: not a valid DFS acl
```

Mit der ursprünglichen Zelle ist der `foreign_user`-Eintrag nicht gültig. Er muss also vorher gelöscht werden:

```
dcecp> acl modify testdir -remove \
> {foreign_user ../../dce.uni-muenster.de/suselbe}
dcecp> acl modify testdir -cell ../../dce.uni-muenster.de
dcecp> acl show testdir -cell
../../dce.uni-muenster.de
```

Wenn ein Benutzereintrag in der voreingestellten Zelle der ACL nicht aufgelöst werden kann, dann sieht der Eintrag folgendermaßen aus:

```
dcecp> acl modify testdir -add {user swm rw}
dcecp>acl modify testdir -cell {../../dce.uni.stuttgart.de}
dcecp> acl show testdir
{mask_obj rw----}
{user_obj rwxcid}
{user 000029a4-83df-21cf-8b00-02608c2ec623 rw----}
{group_obj -----}
{other_obj -----}
```

Es handelt sich dabei um die globale numerische Benutzerkennung, auch **UUID** (*unique universal identifier*) genannt.

Dies verdeutlicht noch einmal die Problematik des „Verschenkens“ von ACLs an fremde Zellen.

Literatur

- [1] Transarc DCE: Introduction to DCE
- [2] Transarc DCE: DFS Administration Guide Version 1.1
- [3] Solaris 2.5.1: System Administration Guide, Volume II.

(Fortsetzung in der nächsten **infoRUM**-Ausgabe)

RUM-Lehre

Lehrveranstaltungen im Wintersemester 1998/99

**Beratung zum
Lehrangebot durch
Herrn W. Bosse,
jeweils Di, Do 11-12,
Tel. 83-3 15 61**

320063	Kommunikation und Information im Internet ⁴ Mo 11 – 13 Hörsaal: M2, Beginn: 19.10.1998	Mertz, K.-B.
320078	Publizieren im Internet mit HTML Mi 15 – 17 Hörsaal: M4, Beginn: 21.10.1998	Neukäter, B.
320082	Programmieren in Java Mi 9 – 11 Hörsaal: M4, Beginn: 21.10.1998	Sturm, E.
320097	Objektorientiertes Programmieren in C++ Di 13 – 15 Hörsaal: M4, Beginn: 20.10.1998	Mersch, R.
320101	Programmentwicklung in Pascal unter Delphi Di 15 – 17 Hörsaal: Raum 107, Einsteinstr. 60, Beginn: 20.10.1998	Pudlatz, H.
320116	Einführung in Mathematica Di 15 – 17 Hörsaal: M2, Beginn: 20.10.1998	Süselbeck, B.
320120	Statistische Datenanalyse mit dem Programmsystem SPSS Mi 11 – 13 Hörsaal: M4, Beginn: 21.10.1998	Nienhaus, R.
320135	Einführung in Windows NT ⁴ Fr 10 – 12 Hörsaal: Raum 206, Röntgenstr. 13, Beginn: 23.10.1998	Kämmerer, M./ Kamp, M.
320140	Einführung in Unix Do 13 – 15 Hörsaal: M2, Beginn: 22.10.1998	Grote, M.
320154	Rechnernetze: Technische Grundlagen Do 10 – 12 Hörsaal: Raum 206, Röntgenstr. 13, Beginn: 22.10.1998	Richter, G./ Schulze, D./ Speer, M./ Wessendorf, G.
320169	Kolloquium des Zentrums für Informationsverarbeitung Fr 13 – 15 Hörsaal: M4, Beginn: nach Vereinbarung	Held, W.

⁴ Wegen der Begrenzung der Teilnehmerzahl ist für diese Veranstaltung eine Anmeldung im Dispatch des Zentrums für Informationsverarbeitung (Universitätsrechenzentrum) erforderlich.

Kommentare zu den Veranstaltungen

320063 Kommunikation und Information im Internet

In den letzten Jahren haben sich die internationalen Datenkommunikationsnetze, eines der wichtigsten ist das Internet, in rasantem Tempo ausgebreitet. Sie sind durch ihre Möglichkeiten zur Informationsgewinnung und zur Kommunikation ein unverzichtbares Hilfsmittel – nicht nur für Wissenschaftler.

Den Teilnehmern der Veranstaltung wird in praktischen Übungen gezeigt, wie man sich in dieser komplexen Welt zurechtfinden und sie sich zunutze machen kann. Vorausgesetzt werden nur elementare Kenntnisse im Umgang mit Computern.

320078 Publizieren im Internet mit HTML

Neben den traditionellen Medien Buch, Zeitschrift, Presse, Rundfunk und Fernsehen wird das Internet zunehmend zur Veröffentlichung wissenschaftlicher Erkenntnisse in Wort, Bild und Ton genutzt. Eine wichtige Grundlage für Veröffentlichungen im Internet ist die Hypertext Markup Language (HTML), mit deren Hilfe ein Geflecht von Texten, Bildern und anderen multimedialen Elementen im World Wide Web (WWW) dargestellt werden kann.

Die HTML steht im Mittelpunkt dieser Vorlesung, in der gezeigt werden soll, dass es keiner besonderen Rechner- oder Informatikkenntnisse bedarf, um Web-Seiten für das Internet zu gestalten. Voraussetzung für diese Veranstaltung sind lediglich Kenntnisse, wie sie etwa in den Vorlesungen „Kommunikation und Information im Internet“ vermittelt werden. Hilfreich sind auch Kenntnisse der rechnergestützten Textverarbeitung, die als Hilfsmittel zur Erzeugung von HTML-Dokumenten eingesetzt werden kann.

Außer der HTML sollen im zweiten Teil der Vorlesung weitere Ausdrucksmöglichkeiten behandelt werden, wie MathML für mathematische Texte und XML, das wie HTML auf den ISO-Standard SGML aufbaut, jedoch flexibler ist und eine größere Klasse von Anwendungen abdeckt.

320082 Programmieren in Java

Java ist eine Programmiersprache, die von SUN Microsystems direkt für das Internet entwickelt wurde. Sie erlaubt es Anwendungen zu schreiben, die vom Benutzer über das Internet angefordert und auf seiner Maschine ausgeführt werden können, ohne dass der Entwickler die lokale Umgebung des Anwenders, wie Hardware und Betriebssystem, kennen muss.

Als objektorientierte Sprache ähnelt Java der Sprache C++, ist jedoch konzeptionell einfacher und enthält spezielle Sicherheitsfunktionen. In Java geschriebene Programme, sogenannte Applets, lassen sich insbesondere zur Gestaltung von WWW-Seiten verwenden, die dynamische Elemente, also z. B. bewegte Bilder, enthalten.

Java hat sich seit einigen Jahren auf dem Markt etabliert, und es ist zu erwarten, dass es sich weiterhin dynamisch entwickelt.

320097 Objektorientiertes Programmieren in C++

Objektorientierte Programmierung hat in den letzten Jahren stark an Bedeutung gewonnen. In dieser weiterführenden Lehrveranstaltung werden die Prinzipien der objektorientierten Programmierung vorgestellt und mit Hilfe der Programmiersprache C++ demonstriert. C++ ist eine Erweiterung der Programmiersprache C um objektorientierte Elemente.

Die Veranstaltung setzt Kenntnisse in der Programmierung mit C voraus.

320101 Programmentwicklung in Pascal unter Delphi

Borland Delphi ist nicht nur eine Programmiersprache für PCs, sondern, wie schon Turbo Pascal und Borland Pascal, eine mächtige Entwicklungsumgebung, die die 32-Bit-Architektur optimal nutzt und daher vorwiegend in der Windows-95/NT-Umgebung eingesetzt wird.

Wie schon das bewährte Turbo Pascal erzeugt der Delphi-Compiler schnellen und kompakten Code. Die anwenderfreundliche grafische Benutzeroberfläche unterstützt die von den Vorgängersystemen her vertraute objektorientierte Programmierung mit in einer mächtigen Unit-Bibliothek vorhandenen Werkzeugen, die Windows-, Datenbank- und sogar Internet-Programmierung erleichtern.

Die Veranstaltung wendet sich an Programmieranfänger, die von Anfang an die Eleganz der strukturierten und objektorientierten Programmierung in einer Windows-Umgebung kennen lernen und einsetzen wollen. Dabei soll zur Vertiefung des Gelernten zu praktischen Übungen angeregt werden. Wegen der damit verbundenen Begrenzung der Teilnehmerzahl ist eine Anmeldung im Dispatch des Rechenzentrums erforderlich.

320116 Einführung in Mathematica

„Mathematica is a system for doing mathematics by computer“. Dieser Satz von Stephen Wolfram, dem Autor des Systems, umreißt schon die wesentlichen Merkmale dieser interaktiven Programmiersprache aus dem Bereich der Computer-Algebra. In der Vorlesung erfolgt zunächst eine Einführung in das symbolische Rechnen. Anschließend werden die vielfältigen Möglichkeiten von Mathematica als Anwendungssystem zur Lösung von Problemen aus Analysis, Linearer Algebra und anderen Gebieten der Mathematik aufgezeigt. Der zweite Teil der Veranstaltung ist dem Thema Visualisierung gewidmet und stellt Mathematica als Grafiksystem vor. Die grundlegenden Techniken von Mathematica als Programmiersprache bilden den letzten Teil des Kurses.

320120 Statistische Datenanalyse mit dem Programmsystem SPSS

Das statistische Programmsystem SPSS (Statistical Package for the Social Sciences) wird in einer aktuellen Windows-Version vorgestellt und erprobt. Mit diesem System stehen bequem aufzurufende Programme zu den gebräuchlichen univariaten und multivariaten statistischen Verfahren sowie zur Datenaufbereitung zur Verfügung. SPSS wird z. B. zur statistischen Auswertung von Fragebögen eingesetzt.

In dieser Veranstaltung wird das programmtechnische Rüstzeug zur Durchführung derartiger Auswertungen vermittelt. Solide Grundkenntnisse bezüglich der anzusprechenden statistischen Verfahren sowie Kenntnisse der Anwendungsmöglichkeiten dieser Verfahren im jeweiligen Fachgebiet sind erwünscht und bei den praktischen Übungen von großem Nutzen.

320135 Einführung in Windows NT

In dieser Veranstaltung werden die grafische Benutzeroberfläche, das Dateisystem und einige Systemprogramme von Windows NT vorgestellt. Zur Erprobung steht den Teilnehmern zusätzlich ein reservierter Übungsraum zur Verfügung. Vorkenntnisse sind nicht, eine Anmeldung ist unbedingt erforderlich.

320140 Einführung in Unix

Unix ist ein weitverbreitetes Mehrbenutzerbetriebssystem. Es ist auf Rechnern verschiedener Hersteller und unterschiedlicher Leistungsklassen ablauffähig. Damit steht dem Unix-Anwender vom Mikrorechner bis zum Großrechner die gleiche leistungsfähige und komfortable Programmier- und Arbeitsumgebung zur Verfügung. Hardware-Unterschiede der einzelnen Maschinen werden weitgehend verdeckt.

FEIG: *Unix von Anfang an*, Fischer

SCHRÖPFER: *Unix*, dtv

HECK: *Standard-Betriebssystem UNIX*, rororo

HECK: *Standard-Betriebssystem UNIX für Fortgeschrittene*, rororo

HARIG: *UNIX im Alleingang*, Springer

320154 Rechnernetze: Technische Grundlagen

Diese Veranstaltung gibt einen Einblick in die technischen Grundlagen der Rechnervernetzung. Folgende Themen werden behandelt:

- Strukturmodell für Kommunikationsfunktionen (OSI-Modell)
- Grobe Struktur des Rechnernetzes der WWU Münster
- LAN-Technik: Ethernet, Fast Ethernet, FDDI
- Routing, Bridging und Switching
- Grundlegende Internet-Protokolle: IP, TCP, UDP, ICMP, ARP, DNS, WINS, DHCP
- Verwendung von Telefonnetzen (analog und ISDN) für die Datenkommunikation: Einwahlsysteme, LAN-LAN-Kopplung
- Neuere Entwicklungen: Funk-LAN, ADSL, ATM, IPv6
- Detaillierte Darstellung der Struktur und Funktion des Rechnernetzes der WWU Münster

320169 Kolloquium des Zentrums für Informationsverarbeitung

Im Rahmen des Kolloquiums werden Vorträge über aktuelle Themen der Informationsverarbeitung gehalten. Vortragstermine werden im WWW und durch Aushang bekanntgegeben.

Liebe(r) Leser(in),

wenn Sie **inforum** regelmäßig beziehen wollen, bedienen Sie sich bitte des unten angefügten Abschnitts. Hat sich Ihre Adresse geändert oder sind Sie am weiteren Bezug von **inforum** nicht mehr interessiert, dann teilen Sie uns dies bitte auf dem vorbereiteten Abschnitt mit.

Bitte haben Sie Verständnis dafür, dass ein Versand außerhalb der Universität nur in begründeten Einzelfällen erfolgen kann.

Vielen Dank!

Redaktion **inforum**



-
- Ich bitte um Aufnahme in den Verteiler.
 - Bitte streichen Sie mich/den nachfolgenden Bezieher aus dem Verteiler.
 - Mir reicht ein Hinweis per E-Mail nach dem Erscheinen einer neuen WWW-Ausgabe.

Meine E-Mail-Adresse:

An die
Redaktion **inforum**
Universitätsrechenzentrum
Einsteinstr. 60
48149 Münster

- Meine Anschrift hat sich geändert.
Alte Anschrift:

Absender:

Name: _____

FB: _____ Institut: _____

Straße: _____

Außerhalb der Universität:

(Bitte deutlich lesbar in Druckschrift ausfüllen!)

Ich bin damit einverstanden, dass diese Angaben in der **inforum**-Leserdatei gespeichert werden (§ 4 DSGVO NW).

Ort, Datum

Unterschrift