



Nutzerservice des Universitätsrechenzentrums

Straße der Nationen 62, Raum 072 (Eingang am Hbf.), Tel. 0371/531-1656
Reichenhainer Straße 70, Raum B405 (Turmbau), Tel. 0371/531-3705
Öffnungszeiten: Mo-Fr 8:45 -- 11:30 Uhr, Mo, Die, Do, Fr 12:45 -- 18:00 Uhr
Helpdesk: hilfe@hrz.tu-chemnitz.de

Wir wünschen allen Nutzern schöne und erholsame Feiertage



sowie Gesundheit, Glück und Erfolg für 2004!

Impressum

Herausgeber:
TU Chemnitz
Universitätsrechenzentrum
Str. der Nationen 62
09111 Chemnitz
Leiter: Prof. Dr. U. Hübner
E-mail: huebner@hrz.tu-chemnitz.de

Redaktion:
Dipl.-Math. Ursula Riedel

Redaktionsbeirat:
Dipl.-Math. Matthias Clauß
Dipl.-Inform. Frank Richter
Dr. Wolfgang Riedel

Redaktionsschluss: 31.10.2003

Anmerkungen: Bezeichnungen hier genannter Erzeugnisse, die auch eingetragene Warenzeichen sind, wurden nicht besonders gekennzeichnet. Eine fehlende Kennzeichnung heißt nicht, dass die Bezeichnung ein freies Warenzeichen ist. Die Beiträge enthalten Links zu anderen Seiten im Internet. Gemäß einem Urteil des Landgerichts Hamburg vom 12. Mai 1998 wird hiermit erklärt, dass wir keinen Einfluss auf die Gestaltung und auf die Inhalte der referenzierten Seiten haben. Wir distanzieren uns hiermit ausdrücklich von allen Inhalten aller referenzierten Seiten.

Mitteilungen des URZ

4/2003

In dieser Ausgabe

- **Windows XP - vom Poolbetrieb zum Administrationsdienst**
- **Windows XP - Authentifizierungstechnologie**
- **Systeminstallation/-verteilung von Windows XP**
- **Wie weiter mit Linux im URZ der TU Chemnitz?**
- **ALI - Automatisches Installationsverfahren für Fedora Linux**
- **HPC: Multiprozessorrechner**
- **Abwehr unliebsamer E-Mails - an drei Fronten gegen Spam**
- **Spam-Filter beim Benutzer: Junk-Mail-Filter in Mozilla**
- **E-Mail-Verteiler mit Mailman**
- **Scheckkartenformat nun auch in der UB**
- **Kurzinformationen**



Windows XP - vom Poolbetrieb zum Administrationsdienst

Ausgehend vom aktuellen Stand der Einführung von Windows XP in zwei Pools wird der neue Administrationsdienst Windows XP für Arbeitsplatz-PCs beschrieben. Neben den Voraussetzungen für die Teilnahme an diesem Dienst wird auch das Verfahren zur Migration von bisher im Administrationsdienst Windows NT integrierten PCs skizziert.

Die seit Anfang September 2003 in zwei öffentlichen Computerpools angebotene Betriebssystemplattform Windows XP scheint von den Studenten und Mitarbeitern der TU Chemnitz angenommen zu sein. Bis Ende Oktober wurden mehr als 1150 verschiedene Nutzer registriert, zum großen Teil mit mehreren Sitzungen.

Man könnte meinen, die Einführung von Windows XP in die Dienstpalette des URZ sei damit abgeschlossen. Dem ist nicht so. Es sind weiterhin Arbeiten sowohl in Bezug auf den Poolbetrieb als auch zur Realisierung des Ausbaus der Windows-XP-Plattform im Rahmen der URZ-Dienste notwendig.

So wurden Anfang Oktober planmäßig alle 32 Pool-PCs mit aktualisierten Installationen versehen, zwecks Erweiterung der angebotenen Software. In diesem Fall wurden Software-Pakete im CAD-Umfeld bereitgestellt sowie mathematische Software. Gleichzeitig wurden einige im Pool-Betrieb festgestellte Probleme behoben. Wobei darauf hingewiesen werden muss, dass die weitaus meisten Aktivitäten zwecks Korrektur, Ergänzung und Anpassung der aktuellen Installationen mittels cfengine-Technologie bei jedem Booten eines PC realisiert werden. Dies betraf zum Beispiel die Installation (Hinzufügen) von mehreren sicherheitsrelevanten Patches in den letzten Wochen.

In Bezug auf die für März 2004 geplante Migration aller Windows-NT-Pools nach Windows XP, sind jedoch seitens aller Windows-Pool-Nutzer weitere Aktivitäten notwendig. Jeder sollte sich diese beiden Fragen beantworten:

- Kann ich meine Arbeiten vollständig mit Windows XP realisieren, oder benötige ich noch Windows NT?
- Können bisher in Windows-NT-Pools durchgeführte Lehrveranstaltungen in den neuen Windows-XP-Pools realisiert werden?

Bitte stellen Sie sich diesen Fragen mit Konsequenz!

Administrationsdienst Windows XP

Das Ziel der zweiten Etappe bei der Etablierung von Windows XP im Dienstespektrum des URZ beinhaltet den Aufbau und die Inbetriebnahme eines Administrationsdienstes. Einen Administrationsdienst Windows NT gibt es schon. Dieser wird durch den neuen Windows-XP-basierten Administrationsdienst abgelöst werden.

Der Administrationsdienst Windows XP wird auf der Basis der Technologien des Windows-XP-Poolbetriebs sowie der seit 1997 gesammelten Erfahrungen mit der Administration von mehreren Hundert Windows-PCs aufgebaut.

Wodurch unterscheiden sich die Anforderungen aus dem Administrationsdienst

gegenüber der Pool-Technologie?

1. *Differente Hardware* - In einem Pool zu administrierende PCs sind weitestgehend identisch, sowohl in der Hardware (PC, Geräte, Bildschirm) als auch den Kapazitäten (RAM, Plattengröße).
2. *Integration von Druckern* - Während von den Pool-PCs genutzte Drucker einer einheitlichen Technologie unterliegen, sind in den Struktureinheiten unterschiedlichste Drucker und Druckertechnologien zu beachten.
3. *Kostenpflichtige Software* - In den Pools sind neben freier Software lizenzpflichtige Applikationen installiert, für die das URZ die Kosten übernimmt. Demgegenüber sind die Lizenzierungskosten für jedes einzelne kommerzielle Softwareprodukt an Arbeitsplatz-PCs durch den Lehrstuhl oder die Fakultät zu tragen. Dies führt zu unterschiedlichen Softwareanforderungen.
4. *Kein Nutzerwechsel* - Im Gegensatz zu Pool-PCs dürfte ein Nutzerwechsel (Anmelden eines anderen Nutzers) an Arbeitsplätzen kaum relevant sein. Dies ermöglicht bzw. bedingt andere Policies (Nutzerrechte).
5. *Keine Vorortbetreuung* - In Pools ist eine eingeschränkte Vorortbetreuung möglich, realisiert über die Einbeziehung von Dispatchern aus den Nutzerservice's. An den verteilten Arbeitsplatz-PCs ist dies nicht möglich.

Beschreibung des Administrationsdienstes Windows XP

Ziel des Administrationsdienstes ist es, den Betrieb und die Benutzung von Rechnern im Campusnetz der TU Chemnitz sicher, effektiv und anforderungsgerecht zu gewährleisten. Mit Hilfe von weitestgehend automatischen Verfahren, die auf diesen aktiv genutzten Rechnern regelmäßig initiiert werden, übernimmt das URZ die Verantwortung für alle Aspekte der Systemadministration auf dem gesamten Rechner.

Die Teilnahme am Administrationsdienst beginnt mit einer Anmeldung und der damit verbundenen Spezifikation der gewünschten Leistungen. Dies beinhaltet auch die Anforderung bestimmter kommerzieller Softwarepakete, für die Lizenzgebühren zu bezahlen sind.

Die im URZ realisierte **Erstinstallation** enthält ein vollständig konfiguriertes und nutzbares Betriebssystem. Ein solcher PC ist in das Campusnetz integriert (Rechnername, IP-Adresse) und enthält spezielle Softwarekomponenten, die für ein sinnvolles Arbeiten am PC notwendig sind. (Während für das Betriebssystem Windows XP Lizenzierungskosten entstehen, sind diese Bestandteile kostenlos.)

Die bereitgestellten **Komponenten** sind:

- pgina zur Authentifizierung (Beschreibung siehe anderen Artikel in diesen URZ-Mitteilungen)
- OpenAFS als Netz-Filesystem
- mozilla als Standard-WWW-Browser
- mozilla-Mail als Standard-Mail-Tool
- OpenOffice als Bürosoftware
- cygwin als Werkzeug-/Programme-Set (ermöglicht die Verwendung von aus der

Linux-Welt bekannten Kommandos, bis hin zur Shell)

Weiterhin wird cfengine - für die automatische Aktualisierung einer Installation- sowie ghost - für die Installation eines Betriebssystems - bereitgestellt. Ghost ist ein kommerzielles Produkt, die Kosten übernimmt das URZ.

Der Rechner kann mit einem Loginkennzeichen des URZ genutzt werden. Mit einer erfolgreichen Anmeldung wird das Netzfilessystem AFS verfügbar gemacht, inklusive des jeweiligen Home-Verzeichnisses. Diese Technologie schließt auch die Möglichkeit ein, sich an anderen administrierten Rechnern oder denen in den öffentlichen Computer-Pools anzumelden. Im Gegensatz zu lokalen Daten werden alle im AFS gespeicherten Daten regelmäßig (einmal täglich) gesichert.

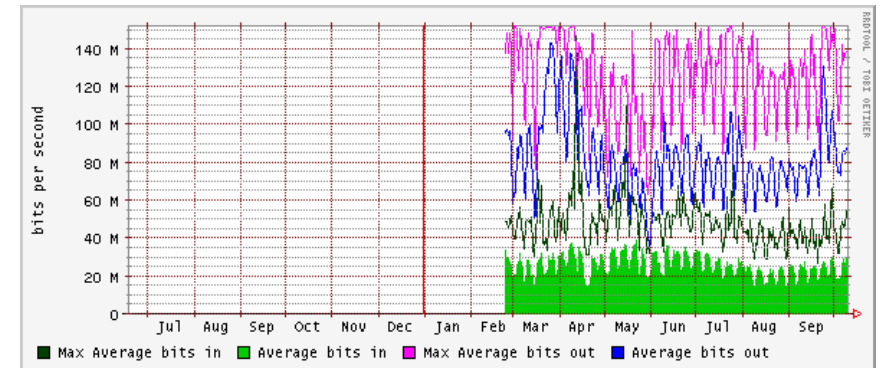
Zusätzliche **Softwareinstallationen**, entsprechend Anforderung, Lizenzierung und Realisierbarkeit, erfolgen im Anschluss an die Erstinstallation über einen Automatismus. (Die eigene Installation von Software ist im Rahmen des Administrationsdienstes nicht möglich.) **Drucker** werden ebenfalls in die lokale Installation integriert, auch übliche Scanner und CD-Brenner.

Leistungen im Rahmen des Administrationsdienstes

- Erstinstallation
- Eine notwendige und zeitnahe Aktualisierung der lokalen Installation bei Auftreten von Problemen, die die Sicherheit der Daten, des Rechners sowie der anderen im Campusnetz existierenden Rechner gefährden.
- Die Wiederherstellung einer nicht mehr funktionsfähigen Installation, einschließlich der Softwarepakete sowie der im Netzfilessystem AFS gespeicherten Daten.
- Aktualisierung oder Ersatz der installierten Software, nach vorheriger Ankündigung.
- Beratung und Unterstützung bei der Nutzung des Rechners einschließlich der angeschlossenen Peripherie.
Notwendige Eingriffe am Rechner werden mit entsprechenden Technologien remote durchgeführt. Führen im Extremfall diese Maßnahmen nicht zum Ziel, wird das Problem im Labor des URZ behoben.
- Die Verfügbarkeit der öffentlich aufgestellten Drucker sowie lokal zu integrierender Drucker (soweit von Betriebssystem und Technologie unterstützt).
- Die Rechte (Zugriffsrechte, policies) sind so gesetzt, dass eine Beeinflussung durch andere Nutzer/Prozesse ausgeschlossen wird.
- Mittels automatischem Monitoring wird versucht, prophylaktisch Maßnahmen zur Sicherung der Funktionsfähigkeit von System und Hardware zu einzuleiten. Eine Überwachung von Nutzerprozessen findet nicht statt.
- Das Netzfilessystem AFS wird über folgende Laufwerke bereitgestellt:
 - Laufwerk H: Home-Verzeichnis des Nutzers
 - Laufwerk K: alle Home-Verzeichnisse
 - Laufwerk U: AFS-Wurzel (weltweites Netzfilessystem)

Änderungen am GWIN-Anschluss

Die Nutzung des Internetzugangs über das Gigabit-Wissenschaftsnetz (**GWIN**) wächst kontinuierlich. In den letzten Jahren reichte es, bei konstanter Bandbreite (155 MBit/s) die monatlich erlaubte Transfermenge einmal im Jahr zu erhöhen. Beginnend in diesem Jahr mussten wir feststellen, dass auch die Bandbreite zum Engpass wird. Aus der Grafik kann man sehen, dass es mehrfach zu Engpässen für den ausgehenden Verkehr kam. Wir mussten teilweise regulierend eingreifen.



Unsere Bemühungen für die Erhöhung der Bandbreite haben inzwischen Erfolg gehabt. Die Bandbreite wird auf **622 MBit/s** erhöht, die monatliche Transfermenge wird jedoch nur auf 12,5 TByte erhöht (jetzt 12). Im Moment erreichen wir die Maximalgrenzen noch nicht, aber bei einer Hochrechnung, ausgehend von der Entwicklung über die vergangenen Jahre, werden wir noch eine Erhöhung der Transfermenge (eingehender Verkehr) etwa Mitte 2004 benötigen.

Günther Fischer, Oktober 2003

Auf der Rückseite befindet sich die Benutzer-Nummer als Barcode:



Unterhalb des Barcodes steht diese Nummer nochmal im Klartext. Somit weiß jeder Benutzer, welche Daten sich in dem Barcode befinden.

Erzeugt werden die Ausweise auf farbigem DIN-A4-Papier, das wir mit bereits vorhandenen duplexfähigen Laserdruckern beidseitig bedrucken. Anschließend werden die Ausweise zwecks einer besseren Haltbarkeit laminiert. Die neuen Ausweise haben die Größe einer EC- oder Kreditkarte, so dass sie nun gut in jedes Portemonnaie passen.

Alle sich zu Beginn des Wintersemesters 2003/2004 neu einschreibenden Studenten und natürlich auch alle anderen neuen Nutzer erhalten ab Oktober 2003 die neuen Ausweise. Schrittweise werden nachfolgend allen bereits angemeldeten Benutzern neue Ausweise ausgestellt. Dieser Aufwand ist auf Grund der geringen Kosten, die pro Ausweis entstehen, sowie der langen Nutzbarkeit gerechtfertigt. Den Nutzern entstehen durch den Umtausch der Ausweise keine Kosten.

Besondere Vorteile der neuen Ausweise sind ihr modernes Design sowie die damit erreichte schnellere Bedienung des Nutzers. Der Bibliothekar greift zum Barcode-Scanner und scannt die Benutzer-Nummer und anschließend mit demselben Gerät die Barcodes der auszuleihenden oder zurückzugebenden Medien. Daraus resultieren eine kürzere Bearbeitungszeit sowie eine geringere Fehlerrate gegenüber der bisherigen manuellen Eingabe der Benutzer-Nummer.

Jan Martin, Holger Trapp, Oktober 2003

Migration von PCs im Administrationsdienst Windows NT nach Windows XP

Der Administrationsdienst Windows XP ist für neue bzw. neu zu beschaffende Rechner vorgesehen, da nur mit solcher Technik die Vorteile von Windows XP auch genutzt werden können. Für die zahlreichen im Administrationsdienst Windows NT existierenden PCs wird das URZ Lösungen anbieten.

Für Ende 2004 ist geplant, den Administrationsdienst Windows NT einzustellen und die für diesen Dienst notwendigen Server (Domain Controller) außer Betrieb zu nehmen. Bis dahin sollen alle im Administrationsdienst Windows NT befindlichen PCs entweder in den Administrationsdienst Windows XP überführt sein (Migration) oder sie werden in die vollständige Verantwortung des jeweiligen Nutzers/Mitarbeiters übergeben.

Die Migrationsmöglichkeit ist abhängig von der technischen Ausstattung des jeweiligen PCs. Dies sind, wie schon in vorhergehenden "Mitteilungen des URZ" veröffentlicht, folgende Mindestvoraussetzungen:

- mindestens 20 GByte Plattenplatz für die ausschließliche Nutzung durch Windows XP
- mindestens 256 MByte RAM
- mindestens 350 MHz CPU

In Bezug auf diese Voraussetzungen muss "**Mindest-**" betont werden. Windows XP benötigt gegenüber Windows NT höhere Kapazitäten, die hier angegebenen RAM- und CPU-Werte sind für eine effektive Nutzung kritisch, natürlich immer abhängig von den eingesetzten Applikationen. Die geforderten 20 GByte Plattenplatz sind anhand der aktuell eingesetzten Softwareprodukte kalkuliert, künftige Anforderungen können auch diesen Wert übersteigen. Im Rahmen von Beschaffungsplanungen sollten also auch diese PCs zur Disposition stehen.

Ablauf der Migration:

1. Noch in diesem Jahr werden die Verträge für den Administrationsdienst Windows NT seitens des URZ gekündigt, mit dem Ziel der Migration zu Windows XP.
2. Beginnend im Januar 2004 werden die Verantwortlichen für in den Administrationsdienst Windows NT integrierte PCs vom URZ angeschrieben werden, zwecks
 - terminlicher Planung
 - Überprüfung der Hardware-Voraussetzungen
3. Abschluss einer Vereinbarung zum Administrationsdienst Windows XP, wenn die Voraussetzungen gegeben sind.
4. Durchführung der Migration oder Überführung durch das URZ

Sind die Voraussetzungen für eine Migration nicht gegeben, wird die Herauslösung aus dem Dienst vorgeschlagen und bis 09/2004 realisiert. Die Maßnahmen zur Überführung in die Eigenverantwortung werden durch das URZ geplant und durchgeführt. Bis zur vollständigen Umsetzung dieser Aktivitäten werden die Windows-NT-Installationen weiterhin aktiv durch das URZ betreut.

Ankündigung: Installationsdienst Windows XP

Für 2004 ist die Einführung eines sogenannten Installationsdienstes Windows XP geplant. Ziel eines solchen Dienstes ist die Unterstützung von Mitarbeitern, deren PCs aus spezifischen Gründen nicht in den Administrationsdienst integriert werden können, die aber trotzdem eine Konfiguration sowie Aktualisierung des PCs durch das URZ nutzen wollen. Neben einer konsistenten und einheitlichen Installation sollen sowohl Komponenten wie OpenAFS oder aktuelle Sicherheits-Patches integriert werden. Die genaue Dienstbeschreibung wird in den nächsten "Mitteilungen des URZ" enthalten sein.

Christoph Ziegler, Oktober 2003

Scheckkartenformat nun auch in der Universitätsbibliothek

Einführung einer neuen, laminierten UB-Benutzerkarte mit maschinenlesbarem Barcode, die durch URZ-Software erstellt wird.

Die in der Universitätsbibliothek im Einsatz befindlichen Benutzerausweise wurden vor über 10 Jahren entwickelt, zwar stets an die Notwendigkeiten angepasst, jedoch nie grundsätzlich überarbeitet. Mittlerweile sind die Ausweise sowohl vom Inhalt als auch vom Format her nicht mehr zeitgemäß.

Es galt daher, einen neuen Ausweis zu kreieren, der vom Format her einer Scheckkarte entspricht und die Benutzer-Nummer auch in maschinell lesbarer Form, d.h. als Barcode enthält.

Auf Grund der angespannten Haushaltssituation und mit Blick auf einen effektiven Einsatz vorhandener Mittel wurde das Ziel verfolgt, den neuen Ausweis so zu gestalten, dass seine Herstellung und Nutzung keine besondere (und meist teure) Hardware erfordern. Des Weiteren musste eine Integration in das bestehende, im März 2003 eingeführte Lokalsystem Libero - auch unter Berücksichtigung der Arbeitsabläufe an den Ausleihtheken - erfolgen. Und schließlich wollten wir eine lokalsystemunabhängige Lösung schaffen, so dass keinerlei Software-Anpassungen im Lokalsystem bzw. in den von uns eingesetzten Zusatzkomponenten notwendig sind.

Der Kauf von ca. 30000 Benutzerausweisen hätte die finanziellen Möglichkeiten der Universitätsbibliothek gesprengt. Außerdem hätte der Ausweisersatz, der ausgestellt werden muss, wenn ein Nutzer seinen Ausweis verliert, die Kosten für die Nutzer enorm gesteigert. Auch dies wollten wir unbedingt vermeiden.

Technische Gründe und zusätzliche, vergleichsweise hohe Kosten sprachen auch gegen die Mitnutzung der TU-Card für die UB-Nutzer, die gleichzeitig TU-Angehörige sind.

Unter Beachtung der genannten Aspekte entschieden wir uns dafür, die neuen Ausweise selbst zu entwerfen und herzustellen.

Sie enthalten auf der Vorderseite sämtliche wichtigen Angaben, so auch die Benutzer-Nummer im Klartext:



Für **Abonnenten/Teilnehmer von Mailing-Listen** sind einige Eigenschaften nun via WWW (<https://mailman.tu-chemnitz.de/>) einstellbar: Bevorzugte Sprache, Auslieferungsmodus (jede Mail sofort oder als "Digest"-Zusammenfassung), Abmeldung (auch kurzzeitig).

Das Abonnement von Mailing-Listen ist sowohl über WWW als auch weiterhin einfach über E-Mail (Inhalt ist egal) möglich:

- Anmelden: E-Mail an listenname-join@tu-chemnitz.de
- Abmelden: E-Mail an listenname-leave@tu-chemnitz.de

Der Anmeldevorgang muss immer bestätigt werden, wozu man eine E-Mail mit Informationen erhält. Die komplette Kommandoübersicht erhält man mit einer E-Mail an listenname-request@tu-chemnitz.de mit dem Inhalt **help**

Administratoren von Mailing-Listen können nun alle Verwaltungsaufgaben via WWW-Browser (mit Passwortschutz) erledigen: <https://mailman.tu-chemnitz.de/mailman/admin/listenname>

- Ein- und Austragen von Mitgliedern und Setzen von Eigenschaften (z.B. Berechtigung zum ungeprüften Senden an die Liste)
- Moderation (Genehmigung der Verteilung einer E-Mail an die Liste)
- Mehrere Listen-Administratoren und Moderatoren sind möglich (nützlich im Vertretungsfall).
- Umfangreiche Optionen: Inhaltsfilter, Spamschutz, automatische Antwort.
- Einstellbare Mini-Homepage einer Mailing-Liste (für Interessenten zum An- und Abmelden).
- Ein Archiv der Listen-Beiträge ist via WWW zugreifbar (falls gewünscht).
- Unterstützung von über 20 Sprachen (einstellbar für Liste und individuell für Benutzer).
- Erkennung von unerreichbaren Abonnenten-Adressen, automatische Löschung möglich.

Die Fülle der Möglichkeiten schlägt sich natürlich in der Komplexität der WWW-basierten Administratorschnittstelle nieder. Einige Hilfen finden Sie im WWW unter <http://www.tu-chemnitz.de/urz/mail/list/admin.html>

Angehörige der TU können eigene Mailing-Listen entsprechend der Benutzerordnung des URZ zu Zwecken der Aus- und Weiterbildung, Forschung und Verwaltung nutzen. Weitere Informationen, z.B. über das Anfordern einer neuen Mailing-Liste, finden Sie im WWW unter <http://www.tu-chemnitz.de/urz/mail/list/>

Frank Richter, Oktober 2003

Windows XP - Authentifizierungstechnologie

Der Artikel beschreibt Auswahl und Einordnung der, im URZ eingesetzten Authentifizierungstechnologie für die Plattform Windows XP. Die eingesetzte Lösung "pGina" sowie damit verbundene Entwicklungen an einem AFS-Authentifizierungs-Plugin werden detaillierter dargestellt.

Im Rahmen der Bereitstellung von PCs in einer Poolumgebung wie den öffentlichen Ausbildungspools werden an die Betriebssystemkonfiguration besondere Anforderungen gestellt. Eine besondere Rolle spielen die Authentifizierung und die Anbindung der Homeverzeichnisse für die Ablage persönlicher Daten.

Anforderungen

Ausgehend von den Erfahrungen im Betrieb der Ausbildungspools und administrierten Mitarbeiter-PCs unter Windows NT ergeben sich neue Anforderungen an die Authentifizierungstechnologie. Das bisher eingesetzte Modell einer Windows-Domain hat zwar eine Reihe von Vorteilen, wenn man vorrangig auf die vom Hersteller angebotenen Technologien und Randbedingungen eingehen kann, erreicht aber in einer heterogenen Umgebung schnell seine Einsatzgrenzen.

Der Einsatz der Nachfolgetechnologie **Active Directory** prägt die Charakteristika der Domain-Technologie noch deutlicher, so dass eine Integration in die vorhandene Infrastruktur (Datennetz, Filesharing, Authentifizierungsdatenbasis) nicht realistisch erscheint. Somit ergeben sich folgende Anforderungen:

- Authentifizierung gegenüber AFS/Kerberos
- Keine Bindung an Windows-Domain

GINA - Windows-Authentifizierung

Der Authentifizierungsmechanismus der Betriebssysteme WinNT, Win2K, WinXP basiert auf GINA (Graphical Identification and Authentication), einer ersetzbaren Bibliothek, welche u.a. die Anmeldung und Passwortverifikation realisiert. *Microsofts Platform SDK* enthält Dokumentationen sowie einige Codeteile für die Entwicklung eigener Authentifizierungsschnittstellen.

Darauf beruhen einige zum Teil frei verfügbare GINA-Replacements.

- Doug Scoular: UNIX Integration GINA replacement
- Nigel Williams: NISGINA
- Naomaru Itoi: NI_PAM
- pGina

Einige dieser Entwicklungen existieren bereits seit einigen Jahren. Weiterentwicklungen sind eher selten zu verzeichnen. Auf Grund der aktuellen Entwicklung und Lizenzierung unter der GPL von **pGina** hat sich das URZ für diese Authentifizierungsbibliothek entschieden. Damit sind spezifische Anpassungen und Weiterentwicklungen möglich. Ein weiterer Vorteil ist das Pluginkonzept für eigene Authentifizierungsmodu-

dule.

pGina - Technologie

pGina stellt zunächst einen Ersatz des Windows-Authentifizierungsmechanismus dar. Damit verbunden wird eine neue grafische Schnittstelle zur Eingabe von Nutzerkennzeichen und Passwort angeboten. Diese Oberfläche ist von der Definition neuer Titeltexthe bis zur Darstellung eines Begrüßungsbildes konfigurierbar.

Die eigentliche Verifikation von Nutzerkennzeichen und Passwort wird an eine Plug-inschnittstelle übertragen. Nach der ersten Installation wird ein sogenanntes Null-Plugin aktiviert, was nur die Funktion von pGina überprüfen lässt. Aktuell werden eine Reihe verschiedener Authentifizierungsplugins zu pGina angeboten. Beispielsweise LDAPAuth, Slashdot-Plugin, POP3-Plugin, NIS-Plugin usw. Diese Plugins sind größtenteils durch Nutzer von pGina entwickelt worden. Unterstützt wird die Pluginentwicklung durch Bereitstellung eines *pGina Plugin SDK* mit Dokumentationen, Spezifikationen, einer Testumgebung und Beispielcode.

pGina - AFS-Plugin

Ausgehend von den Anforderungen nach einer zentralen Authentifizierungsdatenbasis wurde im URZ der TU Chemnitz ein neues pGina-Plugin zur Authentifizierung gegenüber AFS/Kerberos entwickelt. Konkret bedeutet das, dass für die erfolgreiche Anmeldung die Loginkennzeichen-Passwort-Kombination gegenüber der AFS-Zelle des Klienten verifiziert wird. Diesen Test realisiert in der Implementierung die AFS-Funktion `ka_UserAuthenticateGeneral()`. Innerhalb des Plugins werden noch weitere Funktionalitäten erbracht. Zum Beispiel wird geprüft, ob der AFS-Klient läuft.

pGina - Anpassungen

Einer der entscheidenden Vorteile von OpenSource-Entwicklungen ist die Verfügbarkeit des Quellcodes. Erst dadurch ist eine individuelle Anpassung an lokale Gegebenheiten möglich. Obwohl pGina weitgehend konfigurierbar ist, waren noch einige Anpassungen notwendig. Nachfolgend sind die wichtigsten Modifikationen aufgezählt:

- Umsetzung deutschsprachiger Dialoge und Fehlermeldungen
- Anpassung der Nutzerprofil-Technologie auf URZ-spezifische Gegebenheiten
- Festlegen von Homeverzeichnis und Loginscript

E-Mail-Verteiler mit Mailman

Mailing-Listen dienen der Gruppenkommunikation per E-Mail. Zur automatisierten Verwaltung solcher Listen wird nun die Software Mailman eingesetzt, deren Eigenschaften hier vorgestellt werden.

Häufig kommt es vor, dass E-Mails an eine ganze Gruppe von Empfängern gesendet werden müssen, wenn z.B. Einladungen an Interessenten, Mitteilungen an Kollegen oder Diskussionsbeiträge an die Arbeitsgruppe verschickt werden sollen. Das einzelne Versenden der Nachricht an die Adressaten wäre sehr aufwändig, insbesondere dann, wenn dies regelmäßig erfolgen soll. **E-Mail-Verteiler** übernehmen diese "Rundbrieffunktion".

Ein solcher E-Mail-Verteiler besteht aus einer Liste von E-Mail-Adressen, die über einen bestimmten Verteilernamen angesprochen werden. Als Mail-Nutzer hat man 2 Möglichkeiten, diese Funktion zu nutzen:

Im **Adressbuch des Mail-Programmes** können Sie auch Verteilerlisten anlegen. Das ist für Rundschreiben von einem Absender an bekannte Empfänger sehr einfach. Für Diskussionen in einer Gruppe mit häufigen Änderungen ist dies jedoch nicht praktikabel, denn dann müssten alle Teilnehmer diese Listen in ihren Adressbüchern identisch halten.

Komfortabler geht dies, wenn eine **Mailing-Liste** benutzt werden kann. Mailing-Listen (auch Mail-Verteilerlisten oder Distribution lists genannt) sind spezielle E-Mail-Adressen. Wenn man an eine solche Adresse eine Nachricht schickt, wird diese von einem Server automatisch an alle Mitglieder dieser Liste verteilt. Ein solcher Server bietet noch mehr: Mail-Benutzer können sich damit bei Mailing-Listen an- und abmelden und Informationen zu existierenden Mailing-Listen beschaffen. Für Listen-Administratoren stehen zusätzliche Möglichkeiten zur Verwaltung bereit. Jede Mailing-Liste hat (mindestens) einen **Listen-Administrator**, der den Zweck der Liste bestimmt, Richtlinien zur Nutzung festlegt und Eigenschaften der Liste (öffentlich, geschlossen usw.) bestimmt.

Das URZ betreibt seit September 2003 einen Mail-Server mit der List Management Software **Mailman** zur automatisierten Verwaltung von Mailing-Listen. Dieses System löst die bisher eingesetzte Software Majordomo ab, da es wesentlich moderner und flexibler ist.

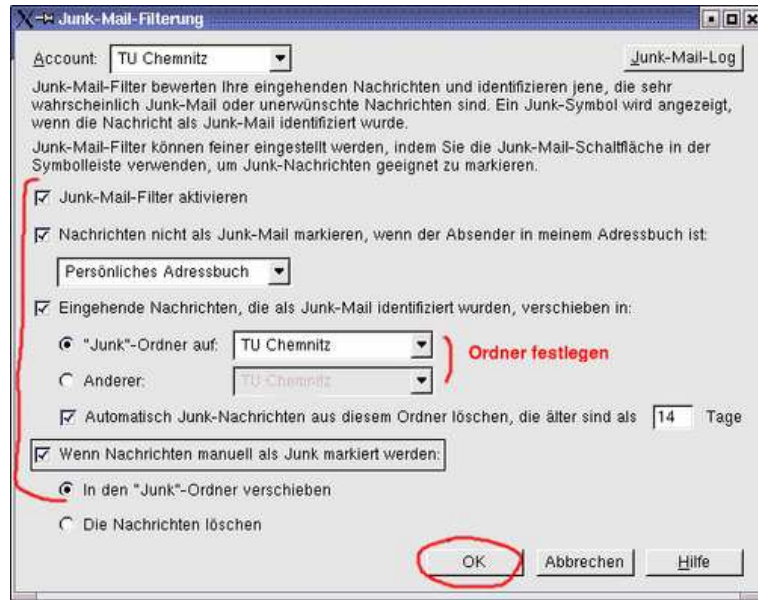
So verwaltete Mailing-Listen werden mit ***listenname@tu-chemnitz.de*** adressiert. Der Listen-Administrator ist erreichbar via ***listenname-owner@tu-chemnitz.de***. Eine jede Mailing-Liste hat eine "Mini-Homepage" mit Informationen für Benutzer: **<https://mailman.tu-chemnitz.de/mailman/listinfo/listenname>**. *listenname* ist jeweils der konkrete Name der Liste. Mailing-Listen werden vom Postmaster der TU angelegt und gelöscht.

Die wichtigsten Eigenschaften von Mailman sind nachfolgend zusammengefasst.


2. Filter wirksam machen:

Wenn Sie mit der automatischen Erkennung zufrieden sind, können Sie den Filter wirksam machen:

In Mozilla-Mail: Menü **Tools | Junk-Mail-Filter...**



Danach werden alle Mails, die als unerwünscht erkannt wurden, in den ausgewählten Ordner verschoben.

Wichtig: Sie sollten regelmäßig in diesen "Junk Ordner" schauen und prüfen, ob dort evtl. auch "gute Mails" gelandet sind. Bei diesen Mails unbedingt wieder das Junk-Mail-Symbol  ausschalten, damit der Filter weiter lernt.

Diese Erkennung basiert auf einem sogenannte Bayesischen Filter, auf den ein Vortrag von Ralph Sonntag eingeht: **Bayes kontra Spam** - <http://archiv.tu-chemnitz.de/pub/2003/0082/> (April 2003).

Frank Richter, Oktober 2003



pGina ScreenShot

Fazit

Durch die enge Bindung des Authentifizierungs-Plugins an AFS ist auf den WinXP-PCs ein funktionsfähiger AFS-Klient sowie eine exakte Synchronisation der Uhrzeit notwendig. Letzteres übernimmt ein freier NTP-Client.

Mit der Realisierung ist die Nutzung der gleichen Authentifizierungsdatenbasis zwischen verschiedenen Systemplattformen (WinXP, Unix, Linux) möglich geworden. Die Entkoppelung der WinXP-PCs vom Domain-Modell macht sich in einer deutlich schnelleren Anmeldung bemerkbar.

Andreas Heik, Oktober 2003

Systeminstallation/-verteilung von Windows XP in Computerpools

Ausgehend von der Aufgabe, eine größere Anzahl PCs gleichzeitig konsistent und schnell mit einer kompletten Windows-XP-Installation zu versehen, werden die Software ghost sowie die Windows-Funktion sysprep vorgestellt. Es werden praktische Erfahrungen vermittelt, beginnend mit einem sogenannten Modell-PC.

Anfang September wurde das Betriebssystem Windows XP in zwei öffentlichen Computerpools bereitgestellt:

- PC-Pool im Raum 066 in der Straße der Nationen 62
- PC-Pool im Raum B302 in der Reichenhainer Straße 70

Vorher musste die Frage gelöst werden, wie 32 PCs möglichst schnell mit der gleichen Installation versehen werden können. Eine manuelle Installation des Betriebssystems sowie der Software auf jedem einzelnen Rechner scheidet generell aus, da bei diesem Verfahren die Gleichheit der Rechner kaum zu gewährleisten ist. Der dafür erforderliche Zeitaufwand wäre ebenfalls ein Vielfaches. Aus diesen Gründen konnte für die Installation der Rechner nur ein Image-Verfahren zum Einsatz kommen. Dazu wurde die Software Symantec Ghost 7.5 genutzt. Der Zeitaufwand für das Verteilen eines Images bleibt so nahezu unabhängig von der Anzahl der betroffenen Rechner. Der Vorteil, dass nach dem Verteilen alle Rechner absolut gleich sind, ist aber nicht überall gewollt. Mit einem Script lassen sich diese Parameter (z.B. Hostname) aber einstellen. Für das Erkennen und Installieren unterschiedlicher Hardware sind ebenso Vorkehrungen zu treffen.

Über Symantec Ghost lassen sich folgende Funktionen realisieren:

- Image-Erstellung einer gesamten Platte oder einer Partition
- Image-Erstellung kann mit Sysprep von Microsoft erfolgen (Hardwareerkennung)
- die Image-Bereitstellung kann lokal oder über Netz erfolgen, (über ein verbundenes Netzlaufwerk oder Ghost-Cast-Server)
- das Verteilen von Images auf mehrere Computer über Multicast
- mit der Ghost-Console können die Rechner zentral verwaltet werden
- wenn mit der Console gearbeitet wird, müssen die Client-Rechner eine freie primäre Partition für die Ghost-Boot-Partition oder einen freien primäre Partitionseintrag für die virtuelle Ghost-Partition haben
- mit dem DOS-Programm GDISK können Partitionen angelegt und gelöscht sowie auch der MBR (Master Boot Record) geschrieben werden

Als Grundlage für die Verteilung musste nun ein sogenannter **Modellcomputer** erstellt werden. Dabei ist zu beachten, dass der Modellcomputer und die zu duplizierenden Computer den gleichen HAL (hardware-abstraction-layer) besitzen. Als Beispiel könnte das jetzt ein ACPI-Uniprozessor-PC sein.

Es besteht aber die Möglichkeit, über Sysprep unterschiedliche Hardware anzupas-


Spam-Filter beim Benutzer: Junk-Mail-Filter in Mozilla

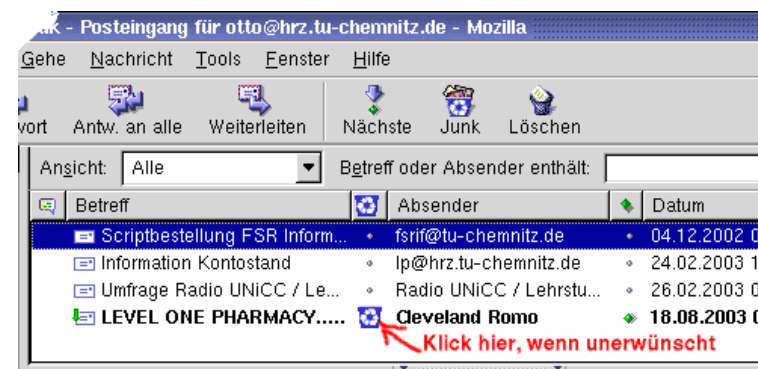
Das vom URZ empfohlene Mail-Programm besitzt Möglichkeiten zur Erkennung von unerwünschten E-Mails. Der Artikel gibt Hinweise zur Benutzung dieses Filters.

Mozillas Mailprogramm enthält ab Version 1.3 einen sogenannte **Junk-Mail-Filter**, der nach einer Anlernphase unerwünschte Spam-Mails erkennt und markiert bzw. gleich in einen anderen Ordner sortiert. Neben den automatischen Schutzfiltern für E-Mail, die für Sie am Mail-Server unerwünschte Mails fern halten, können Sie damit zusätzlich individuell störende Nachrichten filtern.


Bitte beachten Sie folgende Hinweise zur Anwendung der Junk-Mail-Filter in Mozilla.

1. Anlernphase:

Damit der Junk-Mail-Filter" arbeiten kann, müssen Sie ihn **"trainieren"**: Jede Mail, die Sie als unerwünscht ansehen, markieren Sie mit dem Symbol  - Klicken Sie in der Übersicht über Ihren Posteingang entsprechend:



Sie werden bemerken, dass von nun ab Mozilla-Mail von sich aus Nachrichten mit diesem Symbol als "Junk-Mail" kennzeichnet. Sie können die so gekennzeichnete Mail schnell löschen: Menü **Tools | Im Ordner als Junk markierte Mail löschen**

Wichtig: Sollte eine "gute Mail" als "Junk-Mail" gekennzeichnet werden, klicken Sie auf das Symbol , so dass es verschwindet und diese Mail als erwünscht gekennzeichnet wird!

Durch Ihre eigene Klassifizierung lernt Mozilla, welche Mails Sie als erwünscht ansehen und welche Sie lieber nicht haben wollen.

Schließlich sollten Sie **Filtermöglichkeiten Ihres Mail-Programmes** benutzen. Der Artikel "Spam-Filter beim Benutzer: Junk-Mail-Filter in Mozilla" erklärt die individuell mitlernenden Filter für Mozilla-Mail, das vom URZ als Mail-Programm für Windows und Linux empfohlen wird.

Frank Richter, Oktober 2003

sen. Zum Beispiel lassen sich UP-Images auf MP-Computer mit Anpassungen verteilen und umgekehrt. Auch die Verteilung auf unterschiedliche Massenspeichergeräte (IDE-SCSI) ist damit möglich. Das Erkennen unterschiedlicher Netzwerk-, Video- und Audiokarten sollte ebenfalls über Sysprep durchgeführt werden. Dabei können die nicht im Windows vorhandenen Treiber über den Sysprep-Parameter `OemPnPDriversPath` bereitgestellt werden, so dass die Geräte beim ersten Booten erkannt werden.

Die `Sysprep.inf`-Datei sollte alle die Parameter enthalten, die für eine automatische Ausführung des Mini-Setup notwendig sind. Die `Sysprep.inf`-Datei kann mit dem Programm `setupmgr.exe` erstellt und bearbeitet werden. Sysprep stellt weiterhin sicher, dass die SID auf den Zielrechnern eindeutig sind und das der Hostname im Netz nicht schon vorhanden ist. Um mit nur einer Sysprep-Datei auszukommen, lässt man sich die Hostnamen generieren und passt sie später an.

Das Betriebssystem unseres Modellcomputers wurde über eine unbeaufsichtigte Installation (`unattended installation`) aufgespielt. Das hat den Vorteil, dass dieser Vorgang jederzeit mit dem gleichen Ergebnis wiederholt werden kann. Im Anschluss daran wurden Servicepacks und Basissoftware wie AFS, NTP, CYGWIN, Acrobat-Reader, Quicktime, Mozilla, Java, Putty, Ghostscript und Ghostview sowie der Console-Client (Ghost) installiert. Nach der Installation des Console-Client meldet sich der Client mit seiner Konfiguration an der Console. Danach wird die Logon-Methode von `msgina` auf `pgina` umgestellt. Das sollte immer nach der Installation des Console-Clients erfolgen, weil sonst die Konfiguration des Client an der Console nicht eingelesen werden kann. Über `gpedit.msc` wurden die Sicherheitsrichtlinien und Gruppenrichtlinien angepasst.

Danach kann der Vorgang zum Erstellen des Images mit Sysprep an der Ghost-Console gestartet werden. Das Betriebssystem des Modellcomputers wird dabei in einen "Grundzustand" versetzt und davon das Image erstellt. Der Modellcomputer verbleibt nach Beendigung des Image-Vorganges in der Kommunikation mit der Ghost-Console und muss durch Eingabe von `CTRL-C` und `ngctdos -hide` wiederbelebt werden. Danach durchläuft der Modellcomputer ebenfalls das Mini-Setup wie ein anderer Computer, der dieses Image aufgespielt bekommt.

Nach der Erstellung des Images vom Modellcomputer war nun nach einem optimalen Weg für die Verteilung auf die Poolrechner zu suchen. Die Plattenkonfiguration in den beiden Pools stellte sich folgendermaßen dar:

- Pool 066: 2 Platten zu je 40GB
- Pool B302: 1 Platte zu 80GB

In beiden Pools ist Linux und Windows installiert (Dualboot-Systeme). Im Pool 066 war die erste Platte von Windows NT belegt, so dass diese Platte problemlos neu partitioniert werden konnte (damit NT gelöscht) für das Aufspielen der WindowsXP-Partition. Im Pool B302 wurde eine neue größere Platte (80GB) eingebaut. Danach wurden 2 primäre Partitionen zu je 20 GB angelegt (eine für WindowsXP, eine für Reserveplatz, durch späteres Löschen wird der freie primäre Slot in der Partitionstabelle erreicht). In den verbleibenden Platz wurde Linux neu installiert und danach das Modellcomputer-Image.

Für das Verteilen des Images bieten sich folgende Wege an:

- Vorgang über die Ghost-Console gestartet: da diese Rechner mit neu partitionierten Platten (also ohne ein bereits installiertes Windows) vorlagen, wäre eine Ghost-Boot-Partition nötig gewesen. Dieser Weg wurde aus Aufwandsgründen nicht weiter verfolgt. Das unterschiedliche Verhalten der von der Netzwerkkarte abhängigen NDIS-Treiber bestätigte diese Entscheidung.
- Booten der Clients von einer Netzwerkbootdiskette von Ghost und verbinden mit einer bereits gestarteten Ghost-Cast-Sitzung. Die Ghost-Cast-Sitzung kann automatisch gestartet werden (Uhrzeit, Zeitintervall, Clientzahl). Dieser Weg wurde für die Verteilung in den Pools genutzt.

Diese beiden Verfahren nutzen standardmäßig Multicast, wodurch sich die Netzwerkbelastung erheblich reduziert, weil jedes Paket zu einer Gruppe von Rechnern geschickt wird.

Eine weitere Möglichkeit der Systemverteilung, über Diskette zu booten und von einem verbundenen Netzlaufwerk das Image zu holen, wäre nur für eine einzelne Installation sinnvoll.

Beim Verteilen des Images im Pool 066 blieben einige Rechner hängen. Der Gesamtvorgang wurde dadurch nicht beeinträchtigt. Diese Rechner wurden in einem zweiten Versuch zurückgespeichert.

Am Ende des Vorganges zum Aufspielen des Images wird automatisch ein Reboot ausgeführt. Es wird das Mini-Setup durchlaufen (Hardwareerkennung) und wenn alle erforderlichen Parameter in der Datei sysprep.inf bereitgestellt wurden, sind keine zusätzlichen Eingaben notwendig. Aufgrund der Tatsache, dass die Hostnamen automatisch generiert werden, ist ein geringer Umfang an Nacharbeit erforderlich. Voraussetzung für die Automatisierung dieses Schrittes ist, dass die Rechner in DHCP und DNS registriert sind. Über Sysprep wird dem neuen Rechner mitgegeben, sich einmal automatisch als Administrator anzumelden und ein Konfigurationsscript auszuführen. In diesem Script wird aus der über DHCP erhaltenen IP-Adresse der richtige Hostname ermittelt und in die Registry eingetragen. Danach werden die Dienste für den Console-Client und das automatische Aktualisieren/Installieren von Software (mit CFENGINE vergleichbar) gestartet sowie die AFS-Konfiguration modifiziert. Nach der Anmeldung an der Ghost-Console wird die Authentifizierungssoftware pGina aktiviert und der Rechner neu gebootet.

Aus diesem Ablauf ist zu ersehen, dass während dieses Vorganges die Rechner zwei Mal automatisch gebootet werden. Bei Dualbootssystemen empfiehlt es sich, in der Vorbereitung das Standardbootssystem auf Windows einzustellen. Am Ende des gesamten Vorganges stehen dann alle Rechner im Windows und zeigen das Anmeldefenster von pGina. An dieser Stelle kann durch einen Console-Vorgang das Standardbootssystem wieder auf Linux gestellt werden.

Besonders hinweisen möchte ich auf den Schutzfilter **Textanalyse**, womit alle E-Mails von außerhalb durch ein regelbasiertes Erkennungssystem bewertet werden. Aus dem Inhalt der Mail (bis max. 100 KBytes) wird eine "Spam-Bewertung" (Spam score) berechnet. Aktivieren Sie diesen Schutz, werden für Sie Mails mit der "Spam-Bewertung" > 7 geblockt. Wer diesen Schutz nicht einschaltet, bekommt weiterhin alle Mails. Anhand des Headers `X-Spam-Score` kann individuell gefiltert werden.

Es liegt auf der Hand, dass die Installation und Betreuung dieser Schutzmaßnahmen vor Spam für das URZ einen nicht zu vernachlässigenden Aufwand bedeutet, den nicht jeder Administrator eines Mail-Servers im Internet aufbringt. So gibt es leider auch Betreiber, die mit dem Thema "Schutz vor Spam" recht nachlässig umgehen (kein Schutz der Mail-Server - "offene Relays") und damit das Problem verschärfen. Das hat verschiedene Ursachen - Mangel an geschultem Personal, kein Geld, keine Zeit ... Dies ist ein Problem, was sich durch Personalabbau und Etatkürzungen verschärft.

3. *Schutzmöglichkeiten der Benutzer*

Einen vollständigen Schutz vor Spam-Mails werden die o.g. Maßnahmen nicht bieten können, zumal die Einschätzung, welche E-Mail denn nun Spam ist, sehr subjektiv ist. Nicht jede Werbung ist für alle von vornherein unerwünscht ...

Als Benutzer von E-Mail sollten Sie einige Regeln beachten:

- **Gehen Sie sorgsam mit Ihrer Mail-Adresse um.** Legen Sie sich für Online-Formulare oder News-Postings evtl. eine extra Adresse zu (z.B. bei kostenlosen Anbietern).
- Beim Senden einer **E-Mail an viele Empfänger:** Verwenden Sie dafür unbedingt das **Bcc** - Feld (Blind-Kopie). Damit vermeiden Sie lange Adress-Listen im Mail-Kopf. Solche leider häufig versendeten "Adress-Sammlungen" sind nicht nur unter den Aspekten des Spam-Schutzes ein Problem, sondern können auch aus geschäftlichen Gründen sehr problematisch sein, wenn es sich z.B. um eine komplette Kundenliste handelt.
- Natürlich sollten Sie niemals eigene Massen-Mails senden oder sich an Kettenbriefen beteiligen.

Wenn Sie Spam-Mails empfangen:

- **Nicht** auf enthaltene Verweise **klicken**, keine E-Mail zum "Abmelden" zurück schicken.
- Immer gilt: **Vorsicht vor ungefragt mitgesendeten Anhängen** - niemals ungeprüft öffnen (Virengefahr - aktuelles Antivirenprogramm verwenden)!
- Informieren Sie sich über Filtermöglichkeiten Ihres Dienste-Anbieters (für TU Chemnitz siehe 2.).

Abwehr unliebsamer E-Mails - an drei Fronten gegen Spam

Unerwünschte E-Mails sind leider zu einer Massenplage geworden. Der Artikel reißt an, auf welchen Gebieten etwas gegen Spam unternommen werden muss, und zeigt, welche Schutzmöglichkeiten E-Mail-Nutzer der TU Chemnitz nutzen können.

Die Nutzbarkeit von "Electronic Mail" ist zunehmend bedroht durch verantwortungslose Versender von ungezielten Massen-Mails, die unsere Mailboxen mit ihren meist dubiosen Nachrichten überfluten. Diese unerwünschten Mails werden als Spam oder "Junk Mail" bezeichnet.

Es gibt drei Bereiche, in denen gegen diese unliebsame Erscheinung in der elektronischen Kommunikation gearbeitet wird.

1. Bemühen auf juristischer und politischer Ebene

Die Medien berichten von Klagen großer Internet-Provider gegen Versender von Spam-Mails in den USA mit hohen Schadensersatz-Forderungen. In der EU wurde 2001 das "E-Privacy Directive Proposal COM(2000) 385" verabschiedet: "Commercial Email in European Economic Area will not be allowed without recipients' prior consent." Bis Ende 2003 soll dies in nationale Gesetze umgesetzt sein.

Nunja, wenn dies dann auch durchsetzbar ist, wäre uns allen geholfen ... Wegen der weltweiten Ausbreitung des Internets und der meist schwierigen, aber nicht unmöglichen Rückverfolgung des Absenders werden nationale Gesetze allein das Spam-Problem nicht beseitigen. Hoffen wir wenigstens auf eine Eindämmung.

2. Anstrengungen auf Seiten der Infrastruktur-Betreiber

Die Administratoren von E-Mail-Servern stecken in einer Zwickmühle: Auf der einen Seite verbietet das Post- und Fernmeldegeheimnis, persönlich adressierte Nachrichten zu verwerfen oder zu verändern. Andererseits möchten verantwortungsbewusste Betreiber die Benutzerinnen und Benutzer vor diesen Mails mit unerwünschten und gar gefährlichen Inhalten schützen.

An der TU Chemnitz versuchen wir diesen Konflikt zu lösen, indem wir eine Reihe von Schutzmöglichkeiten anbieten, die jeder Benutzer individuell nutzen kann, aber nicht muss. Für neu eingerichtete Mail-Benutzer werden bereits Schutzfilter gesetzt. Darüber informiert eine Nachricht in der neuen Mailbox.

Diese Möglichkeiten wurden in den "Mitteilungen des URZ" des öfteren vorgestellt. Unter <http://www.tu-chemnitz.de/urz/mail/filter> ist nachzulesen, welche Schutzfilter es gibt und wie diese an- oder abzuschalten sind. Gleichzeitig finden Sie dort eine Kontrollmöglichkeit, mit der Sie einen Überblick über evtl. abgewiesene E-Mails erhalten.

Zur Zeit ist die Windows-Partition mit 8,6 GB belegt. Das hochkomprimierte Abbild dieser Partition verbraucht 3,5 GB. Diese Datenmenge muss über das Netz an die Rechner übertragen werden, was ca. 15 min in Anspruch nimmt. Einschließlich vor- und nachbereitender Arbeiten kann so in einer Stunde ein Pool neu mit Windows installiert werden. Probleme bestehen noch dort, wo ein Firewall-Router die Verbindung zwischen Ghost-Server und Client unterbricht und nicht zwingend Unicast verwendet wird.

Karl-Heinz Arnold, Oktober 2003

Wie weiter mit Linux im URZ der TU Chemnitz?

Die Firma Red Hat hat im September angekündigt, die Consumer-Version seiner Linux-Distribution aufzugeben und als **Fedora Project** in die Hände der "Linux-Community" zu geben. Welche Konsequenzen hat das für die bisherigen Nutzer und Betreiber von Red Hat Linux? Der Artikel beschreibt die geplante Vorgehensweise im URZ der TU Chemnitz.

Linux ist eine strategische Betriebssystem-Plattform. Der Einsatz von Linux-Systemen an der TU Chemnitz erstreckt sich über unterschiedliche Server-Bereiche, Mitarbeiter-Arbeitsplätze und Ausbildungs-Pools. In einigen Einrichtungen der Uni werden spezielle Cluster-Lösungen unter Linux eingesetzt, darunter das **Chemnitzer Linux Cluster** (CLiC).

Die Bedeutung von Linux als BS-Plattform wird auch durch die Anzahl der eingesetzten Rechnersysteme sichtbar: allein durch das URZ werden ca. 1300 Linux-Rechner (Stand Ende 2003) betrieben.

Im URZ wurde in der Vergangenheit konsequent auf die Distributionslinie von Red Hat orientiert. Nachdem die Firma Red Hat vor einigen Wochen ankündigte, in Zukunft keine frei verfügbaren Linux-Distributionen mehr bereitzustellen, sondern das bisherige Red Hat Linux als Open Source Projekt (Fedora Project) in die Hände der "Linux-Community" zu geben, entstand zunächst einige Verunsicherung unter den Betreibern (und Nutzern) von Red Hat Linux.

Auch unter den MitarbeiterInnen des URZ wurde intensiv diskutiert, welche Konsequenzen sich aus dieser Entwicklung für den Einsatz von Linux im Desktop- und Serverbereich ergeben. Insbesondere aus folgenden Gründen haben wir uns entschieden, bei Arbeitsplatz- und Poolrechnern auf **Fedora Core 1** (FC 1) zu wechseln (Fedora Core 1 Release Note):

- FC 1 entspricht praktisch der noch von Red Hat vorbereiteten Distribution **Red Hat Linux 10** (deren Einsatz ursprünglich geplant war).
- Man kann nicht sicher sein, dass der Umstieg auf einen anderen *professionellen* Linux-Anbieter (z.B. SuSE, Mandrake) jene Sicherheit bietet, die man sich als Betreiber wünscht, ganz abgesehen von den Problemen, die ein solcher Umstieg mit sich bringen würde.
- Wir haben den Eindruck, dass sich das **Fedora Projekt** recht schnell konsolidiert hat, was sich u.a. auch dadurch ausdrückt, dass die Pflege wichtiger Red Hat Distributionen gesichert werden soll (Fedora Legacy).

Wie sieht nun der konkrete Zeitplan aus? Der Übergang auf FC 1 soll in drei Etappen geschehen:

herkules wurden Lizenzen für die aktuelle Version der Intel-Compiler für C/C++ und Fortran beschafft. Diese Compiler sind bekannt dafür, perfekt an diese CPUs angepasst zu sein und hervorragend optimierten Code zu produzieren. Dabei versuchen sie so kompatibel wie möglich zum Gnu C-Compiler (`gcc`) zu sein.

Weitere Software ist in Vorbereitung, bitte beachten Sie dazu die Informationen auf den entsprechenden Webseiten des URZ. Bei Wünschen oder Fragen zu Compilern, Bibliotheken oder systemnahen Problemen können Sie sich an den Autor dieses Artikels wenden, für Simulations- und allgemeine Mathematik-Software ist Jürgen Winkler zuständig. Wir beide sind telefonisch unter Hausanschluss 1725 zu erreichen.

Nutzung

Die beiden Computerver **herkules** und **medusa** werden genauso wie das Linux-Cluster CLiC über unser Batchsystem PBS bereitgestellt und verwaltet. Zur Anwendung kommt dabei erstmalig eine Weiterentwicklung des bisher im Einsatz befindlichen OpenPBS: *Scalable OpenPBS*. Diese Variante enthält einige Modifikationen zur Verbesserung der Stabilität und Zuverlässigkeit, ist dabei aber voll kompatibel zu OpenPBS und sieht für den Nutzer nicht anders aus. Falls nicht noch unerwartete Probleme auftreten, ist auch mit einem zukünftigen Einsatz auf dem CLiC zu rechnen.

Zur Nutzung der beiden beschriebenen Systeme sind alle Nutzer berechtigt, die bereits Zugang zum CLiC haben, also Mitglied eines angemeldeten Projekts sind. Zusätzliche Interessenten können natürlich ein neues Projekt anmelden. Alle Informationen zum High-Performance Computing an der TU Chemnitz, den hier erwähnten Rechnern und Softwarepaketen sowie zum Zugang können Sie über das HPC-Portal des URZ finden: www.tu-chemnitz.de/urz/hpc

Karsten Petersen, Oktober 2003

Selbstverständlich sind beide Rechner mittels Gigabit-Ethernet ans Campusnetz angeschlossen und auch das AFS kann auf beiden wie gewohnt genutzt werden.



Die beiden Systeme: **herkules** (oben) und **medusa**

Von besonderem Interesse für "leistungshungrige" Benutzer sollten die speziellen Fähigkeiten der beiden CPU-Typen sein.

Die im *herkules* verwendeten Xeon Prozessoren unterstützen mit SSE-2 (*Streaming SIMD Extensions*) die parallele Anwendung einer Operation auf mehrere Fließkomma-Operanden, so können z.B. gleichzeitig vier Zahlen einfacher Genauigkeit mit vier anderen multipliziert werden. Ebenso unterstützen diese CPUs eine virtuelle "Verdopplung" namens *Hyperthreading*; dazu stellt sich eine physikalische CPU dem Betriebssystem gegenüber als zwei CPUs dar und stellt ihre Leistung beiden virtuellen CPUs zur Verfügung. Somit scheint der *herkules* nicht nur zwei sondern vier CPUs zu besitzen. Zwar erhöht dies nicht die reine Rechenleistung der CPUs, doch falls ein Prozess eine "CPU-Hälfte" durch einen langsamen Speicherzugriff blockiert, kann so lange die andere Hälfte arbeiten und damit diese eigentlich verlorene CPU-Zeit nutzen.

Die Itanium 2 CPUs der *medusa* basieren auf einem völlig anderen Ansatz als die sonst üblichen CPUs (es werden z.B. sogenannte VLIW-Befehle verwendet, *Very Long Instruction Word*), dies verleiht ihr eine enorme Leistungsfähigkeit bei niedriger Taktrate, erhöht jedoch die Komplexität der maschinennahen Programmierung ganz erheblich. Zur besseren Ausnutzung der Hardware-Spezialitäten von *medusa* und

1. Einsatz auf (einigen) URZ-Arbeitsplatzrechnern (bis Anfang Dezember).
2. Bereitstellung auf allen vom URZ administrierten Arbeitsplatzrechnern (bis Februar 2004).
3. Installation auf allen Poolrechnern einschließlich der öffentlichen Computerarbeitsplätze der Universitätsbibliothek (Semesterpause, März 2004).

Bei den im URZ eingesetzten Linux-Servern, die gegenwärtig unter RH 7.3 betrieben werden, ist noch nicht klar, ob und wann flächendeckend auf Fedora übergangen wird. Das hängt insbesondere von den Erfahrungen des Einsatzes von FC 1 im Desktop-Bereich ab. Wichtige Kriterien sind dabei die Stabilität und Sicherheit des Systems. Nur wenn gesichert ist, dass ein stabiler, sicherer (und effektiver) Server-Betrieb gewährleistet ist, werden wir auf Fedora Linux wechseln. Eile ist für eine solche Entscheidung aus unserer Sicht nicht geboten, da im Rahmen der oben erwähnten Fedora Legacy die Bereitstellung von Security-Patches für RH 7.3 zumindest bis Ende 2004 gewährleistet werden soll.

Da ähnliche Fragestellungen sicher auch in anderen Einrichtungen der Universität existieren, erscheint es sinnvoll, dass die bisherigen Betreiber von Red Hat Linux einen engen Informations- und Erfahrungsaustausch pflegen. Initiiert wurde dieser auf dem Oktober-UNIX-Stammtisch des URZ, auf dem Enrico Scholz (Informatik-Student und Fedora-Aktivist) zum Stand und der Zukunft des Fedora Projektes berichtete (Enrico Scholz: Das Fedora Projekt - quo vadis Red Hat).

Die weiteren Aktivitäten werden unter Einbeziehung der Erfahrungen mit FC 1 abgeleitet. Diese Erfahrungen und Erkenntnisse werden wir publizieren (Web, Wiki). Geplant ist auch, ein (oder mehrere) Treffen zu organisieren, auf denen in Form von Workshops oder Diskussionsrunden die Möglichkeit des Erfahrungsaustausches besteht.

Matthias Clauß, Oktober 2003

ALI - Automatisches Installationsverfahren für Fedora Linux

ALI (Kürzel für Automatische Linux Installation) ist ein Dienst zur Installation von Linux-Rechnern. Die Verfahren werden gegenwärtig für die Version Linux Fedora 1.0 vorbereitet. Genutzt werden kann der Dienst ab Anfang 2004.

Nutzer dieses neuen Dienstes des URZ sind Uni-Angehörige, die ein funktionsfähiges Linux-Betriebssystem nutzen wollen, aber die Administration des Systems dann in eigener Regie behalten möchten. Insofern ist dieser Installations-Dienst eine Alternative zu dem Komplett-Administrationsdienst LADM, bei dem die Administrationsverantwortung vollständig beim URZ bleibt.

Da Red Hat seine freie Linux-Distribution an Fedora abgegeben hat, bieten wir diesen Dienst ab Januar 2004 für die Version **Linux Fedora 1.0** an. Diese Distribution wird im URZ Nachfolger des bisher eingesetzten **Red Hat Linux 7.3**.

Hardwarevoraussetzungen sind:

- Platte mit mindestens 15 GB freiem Platz für Linux
- 512 MB RAM
- Prozessor mindestens 500 MHz - besser aber ab 1 GHz
- Netzkarte mit Anschluss an Uni-Netz

Über unten stehenden URL können Sie eine Web-Seite mit der konkreten Dienstbeschreibung erreichen. Außerdem können dort minimale Einstellungen für das zu installierende System gemacht werden. Als Ergebnis entsteht ein bootbares Disketten-Image, von dem nach Speichern auf eine 1.4MB Diskette gebootet und das System ohne weitere Eingaben fertig installiert wird. Vorinstalliert ist auch schon OpenAFS, das an der Uni als verteiltes Filesystem zur Bereitstellung der HOME-Verzeichnisse und anderer uniweit benötigter Daten genutzt wird.

<http://www.tu-chemnitz.de/urz/admin/ali/>

Thomas Koppe, Oktober 2003

HPC: Multiprozessorrechner

Zwei Nachfolgesysteme für den "Superscalarcluster" stellen unseren HPC-Nutzern sehr schnelle CPUs und viel RAM zur Berechnung nicht-paralleler Probleme zur Verfügung.

Zur Beschleunigung aufwändiger Berechnungen gibt es eine Reihe typischer Ansätze:

- Eleganter arbeiten - mit besseren Algorithmen
- Härter arbeiten - mit schnelleren Prozessoren
- Hilfe holen - indem die Aufgabe in parallel berechnete Teilaufgaben zerlegt wird

Das Entwickeln besserer Algorithmen ist dabei Sache der Wissenschaftler, das parallele Berechnen von Teilaufgaben ermöglichen wir mit dem Chemnitzer Linux-Cluster CLiC. Für manche Aufgaben eignen sich jedoch beide Vorgehensweisen nicht, oft bedingt durch den Einsatz kommerzieller Software oder aufgrund der prinzipiellen Charakteristika der Aufgabe.

Um auch in diesen Fällen Unterstützung bieten zu können, wurde 1996 unser *Superscalarcluster* aus zwei HP 9000 Systemen mit je vier CPUs und 3,75 GB RAM in Betrieb genommen. Wie nicht anders zu erwarten, sind auch diese Rechner in die Jahre gekommen und entsprechen nicht mehr aktuellen Anforderungen. Daher begannen wir bereits im vergangenen Jahr mit der Planung für Nachfolgesysteme. Nach Installation und ausführlicher Testphase stehen nun zwei neue Computerserver zur Verfügung.

Hard- und Software

Beide Rechner verfügen über jeweils zwei sehr schnelle CPUs und einen großen Hauptspeicher, sind im Detail aber sehr unterschiedlich:

- **herkules:**
 - zwei Intel Xeon CPUs mit jeweils 2.40 GHz und Hyperthreading
 - 6 Gigabyte RAM
 - etwa 46 Gigabyte Platz für temporäre Daten (*Scratch*)
 - Red Hat Linux 7.3, wie auch sonst im URZ
- **medusa:**
 - zwei Intel Itanium 2 CPUs mit jeweils 1.00 GHz
 - 12 Gigabyte RAM
 - etwa 18 Gigabyte Platz für temporäre Daten (*Scratch*)
 - Red Hat Linux Advanced Workstation 2.1AW (entspricht etwa Red Hat Linux 7.2)