



Mitteilungen des URZ

4/2004

In dieser Ausgabe

- A Toolbox for System Configuration and Administration (ToSCA)
- Sicheres Programmieren mit PHP (Teil 3)
- „Nutzerforum des URZ“ - Neue Veranstaltungsreihe
- IP-Adressvergabe
- Windows XP Service Pack 2 - Erfahrungen im URZ
- Adobe-Rahmenvertrag
- Kurzinformationen
- Software-News



A Toolbox for System Configuration and Administration (ToSCA)

*ToSCA ist das Kürzel für **T**oolbox for **S**ystem **C**onfiguration and **A**dministration. ToSCA ist ein System von Datenstrukturen, Verfahren und Methoden zur effektiven und skalierbaren Systemadministration von Rechnern unterschiedlicher Systemplattformen. Der Artikel erläutert die Notwendigkeit einer solchen Entwicklung und gibt einen Einblick in einige Konzepte und Komponenten.*

Motivation

Wer einen Computer nutzt - für welche Zwecke auch immer - hat meist auch mit Fragen der System- und Netzwerkadministration zu tun. Bereits die Installation eines Betriebssystems auf einem Rechner gehört zu diesem Aufgabenkomplex. Die Anbindung des Rechners an das Internet, das Einspielen von Anwendungssoftware, die Beseitigung von Sicherheitslücken, all das sind typische - aber bei weitem nicht alle - Aufgaben der System- und Netzwerk-Administratoren (im folgenden SysAdmins genannt). Wenn ein Nutzer solche Arbeiten an "seinem" Rechner zu erledigen hat (vorausgesetzt er hat das erforderliche Know-How ;-), geschieht das im Regelfalle dadurch, dass er sich über grafische Oberflächen, Web- oder Menü-Schnittstellen "durchhangelt", die entsprechenden Knöpfe (Buttons) anklickt bzw. abgefragte Informationen über die Tastatur eintippt. Diese Vorgehensweise ist zeitaufwändig, wird jedoch meist ohne Klagen in Kauf genommen, wenn am "Ende" der Bemühungen ein funktionsfähiger Rechner bereitsteht. Besteht die Aufgabe darin, nicht nur einen, sondern mehrere Rechnersysteme (Pool, Cluster, Arbeitsgruppe) zu administrieren, spielt der Faktor Zeit schon eine größere Rolle. Vermutlich geht das Eintippen und Klicken wegen des Routineeffektes etwas schneller, aber insgesamt multipliziert sich der Zeitaufwand mit der Anzahl der zu betreuenden Rechnersysteme. Außerdem besteht die Gefahr, dass sich die Systeme im Detail unterscheiden, selbst wenn sie identisch konfiguriert sein sollten: wer ist schon in der Lage, die "per Hand" durchgeführten Aktionen exakt zu wiederholen?

Möglicherweise ist eine solche Vorgehensweise für einige wenige Rechnersysteme hinsichtlich Aufwand und Konsistenz noch akzeptabel. Wie aber sollte man vorgehen, wenn *sehr viele* Rechner betreut werden müssen? An der TU Chemnitz sind gegenwärtig annähernd 10000 (zehntausend) Rechnereinheiten im Einsatz, davon werden ca. 2000 durch MitarbeiterInnen des URZ administriert. Bei solchen Stückzahlen ist eine grundsätzlich andere Vorgehensweise als die oben skizzierte erforderlich - das Zauberwort heißt **Automatisierung**.

Tatsächlich drängt sich hierbei der Vergleich mit unterschiedlichen Modellen der Warenproduktion auf: einerseits der kostenintensiven (Hand-)Fertigung einer kleinen Anzahl eines bestimmten Produktes mit individuell ausgeprägten Eigenschaften, und andererseits der kostengünstigen Massenproduktion mit eher begrenzter Individualisierungsvielfalt. Möglicherweise ist das erste Modell für den Produzenten befriedigender (für den zahlungskräftigen Kunden sowieso). Die Notwendigkeit der Massen-

produktion ergibt sich vornehmlich aus ökonomischen Gesichtspunkten, minimiert werden sollen die einschlägigen Kostenfaktoren, insbesondere die Personalaufwendungen.

Im Bereich der System- und Netzwerkadministration gibt es wenig SW-Lösungen, die sich solchen Zielstellungen verschreiben. Existierende SW-Produkte sind entweder nicht bezahlbar oder für die Anforderungen höherer Bildungseinrichtungen nicht geeignet (oder beides).

ToSCA ist eine Entwicklung des URZ mit der Zielstellung, die Betriebskosten von Rechnersystemen sowie den erforderlichen personellen Aufwand bei der systemseitigen Betreuung dieser Rechner zu reduzieren.

Wesentliche Entwurfsziele

Unterstützung unterschiedlicher Betriebssystemfamilien und Systemplattformen

Grundsätzlich ist der ToSCA-Ansatz offen für verschiedenste *Betriebssystemfamilien*, seien es die zur Familie Linux gehörenden relevanten Linux-Distributionen oder die aktuellen (und zukünftigen) Betriebssysteme von Microsoft (z.B. WXP, W2000, W2003). Das bedeutet nicht, dass SysAdmin-Dienste durch das URZ für alle Distributionen und BS-Versionen bereitgestellt werden. Im konkreten Fall ist das von einer Reihe von Aspekten abhängig, auf die hier nicht weiter eingegangen werden soll.

Unter *Systemplattform* versteht man die Kombination von HW-Architektur und Betriebssystem einer bestimmten Version. Beispiele für unterschiedliche Systemplattformen sind

- Windows XP für Rechner mit 32-Bit-Intel-Architektur (Bezeichnung in ToSCA: WXP_5.1_X86)
- Linux Fedora Core 3 für Rechner der Architektur AMD Athlon 64 (FC_3_x86_64)
- Scientific Linux 3.0.3 für Intel Itanium IA64 (SL_3.0.3_ia86)

Auch hier hilft zum Verständnis eine Analogie aus der "realen Welt": Verschiedene Betriebssystemfamilien entsprechen unterschiedlichen Auto-Herstellern, während eine Systemplattform einem konkreten Modell eines bestimmten Herstellers entspricht. Es ist offensichtlich, dass sich für den Benutzer (Fahrer) vergleichsweise geringe Unterschiede ergeben, während SysAdmins (KFZ-Techniker) spezielle Fähigkeiten und Erfahrungen für jede Systemplattform (jedes zu reparierende Modell) benötigen. Hierbei gilt: die Details bestimmen Unterschied und Aufwand.

Insofern ist die Kategorisierung in Betriebssystemfamilien und Systemplattformen ein Ansatz, um die bei der Systemadministration existierenden Unterschiede/Abweichungen in geeigneter Weise abzubilden.

Skalierbarkeit hinsichtlich Anzahl der Rechner und der Einsatz-Vielfalt

Der Personalaufwand steigt mit jedem weiteren zu betreuenden Rechner. Insofern müssen die eingesetzten Verfahren skalieren, d.h. sie müssen weitgehend automatisiert und der Anteil der "Handarbeit" minimiert werden. Die funktionellen Besonderheiten der Rechnersysteme (dedizierte Serverfunktionalität, spezielle SW usw.) sind weitere Faktoren, die die Skalierbarkeit beeinflussen. Den vergleichsweise geringsten Betreuungsaufwand verursachen Pools oder Cluster mit gleicher Hardware- und SW-Konfiguration.

Die Automatisierung selbst muss einigen Anforderungen genügen. Die wichtigste besteht darin, dass die Verfahren hinreichend abstrakt und allgemeingültig sind und sich somit **generisch** auf konkrete Rechner oder Rechnerklassen anwenden lassen.

Unterstützung kooperativer Systemadministration

Außer den SysAdmins für die jeweiligen Betriebssystemfamilien sind noch eine Reihe von Personen an Admin-Aufgaben beteiligt. Einerseits sind das die "Spezialisten" für bestimmte Sachgebiete, z.B.

- Hardware
- Netzwerk-Sicherheit
- Desktop-Konfiguration
- Druckdienste
- Nutzerverwaltung, Identity-Management

Hinzu kommen die Verantwortlichen für spezielle Funktionen und Dienste, z.B.

- Netzdienste
- Datenbank-Dienste
- spezielle Anwendungen
- Supercomputing
- Bildungsportal Sachsen (BPS)
- Bildungsmarkt Sachsen (BMS)

um nur einige zu nennen. Da sich die Verantwortungsbereiche der beteiligten Personen zumindest teilweise überlagern, besteht hierbei ein nicht zu unterschätzendes Konfliktpotenzial. Überschneidungen müssen ebenso vermieden werden wie "Verantwortungs-Lücken", d.h. Bereiche, wo sich keiner verantwortlich fühlt, sondern auf andere verlässt. Um kooperative SysAdmin erfolgreich zu gestalten, bedarf es bei den Beteiligten gewisser Voraussetzungen, üblicherweise mit dem Schlagwort "Teamfähigkeit" umschrieben. Andererseits sollten die zur Systemadministration eingesetzten Verfahren selbst kooperative Sysadmin unterstützen. Die ToSCA-Konzepte wurden speziell im Hinblick auf kooperative Systemadministration entworfen. Schließlich benötigt man für jene Bereiche - wo technische Verfahren nicht greifen - geeignete organisatorische Regelungen und Konventionen (Policies).

Prinzipien der Systemkonfiguration

Im Grunde kann der Zustand eines Rechnersystems über seine Systemkonfiguration beschrieben werden. Die Informationen über die Systemkonfiguration werden in Konfigurationsfiles abgespeichert. Änderungen der Systemkonfiguration werden direkt wirksam oder indirekt, d.h. nach einer bestimmten Aktion, z.B. der Ausführung eines speziellen Skriptes oder Programmes.

Die Konsistenz der Konfigurationsfiles ist letztlich für die korrekte Funktionsweise eines Rechners notwendig. Zwei Konzepte bilden die Grundlage der Systemkonfiguration mittels ToSCA

- hierarchisches Klassenkonzept
- Repositories für Prototypen der Konfigurationsfiles

Klassen

Das Klassenkonzept ermöglicht es, Konfigurationsfiles sowie Aktionen für die zu betreuenden Rechnersysteme übersichtlich und korrekt zu adressieren. Zunächst gehört ein Rechner einer **Systemplattform-Klasse** an, bei Dual-Boot-Rechnern möglicherweise auch einer weiteren. Jedes Rechnersystem wird in genau eine **Funktions-Klasse** eingeordnet, die Funktions-Klassen sind zueinander disjunkt. Z.B. gehören alle Rechner des Ausbildungs-Pools in der Strasse der Nationen, Raum 066 zur Funktionsklasse `FU_POOL_SN_066`

```
FU_POOL_SN_066 = ( atair rigel deneb wega algol arktur capella prokyon  
pollux sirius castor regulus )
```

Um gemeinsame Eigenschaften besser abzubilden, können mehrere Funktionsklassen zu **Verbund-Funktionsklassen** zusammengefasst werden, z.B. alle Pools im Gebäudeteil Straße der Nationen

```
CFU_POOL_SN = ( FU_POOL_SN_066 FU_POOL_SN_207 FU_POOL_SN_203 )
```

Jeder Rechner bildet eine eigene Klasse, die sog. **Host-Klasse**. Damit können rechner-spezifische Konfigurationen realisiert werden. Außerdem gibt es noch die generische Klasse **any**, zu der alle Rechner (Hosts) gehören. Auf diese Weise ist es auf einfache und elegante Weise möglich, Aktionen zu definieren, die für alle Rechner zutreffen.

Repositories

Repositories im Sinne von ToSCA sind Filesystem-Bäume für Prototypen von Konfigurationsfiles. Repositories befinden sich in einem Netzwerkfilesystem und sind von allen aktiven Rechnersystemen lesbar. Für jede definierte Klasse wird ein Repository aufgespannt, es enthält genau jene Prototypen von Konfigurationsfiles, die diese Klasse von anderen Klassen unterscheiden. Dabei gilt für jeden Prototyp:

- finde die allgemeingültigste Klasse
- vermeide identische Prototypen

Der Pfadname eines Konfigurationsfiles in einem Repository ist dabei i.a. identisch zu dem Pfadnamen des Konfigurationsfiles im Systemfilesystem. Ein einfaches Beispiel soll das verdeutlichen. Im Repository für `FU_POOL_SN_066` ist u.a. der Standard-Drucker für (Linux-)Rechner dieses Pools festgelegt.

```
.../FU_POOL_SN_066/etc/cups/lpoptions
```

Dementsprechend stehen diese Konfigurationsinformationen auf jedem Linux-Rechner des Pools unter

```
/etc/cups/lpoptions
```

Änderung der Systemkonfiguration

Änderungen der Prototypen von Konfigurationsfiles können zu einem beliebigen Zeitpunkt an irgendeinem Rechner vorgenommen werden, vorausgesetzt der betreffende SysAdmin hat die notwendigen Zugriffsrechte. Eine Änderung geschieht indirekt, d.h. sie wird auf einem Rechnersystem erst wirksam, nachdem das Prototyp-File auf den Rechner kopiert und evtl. eine zusätzlich erforderliche Aktion durchgeführt wurde (z.B. der Neustart der betroffenen Systemkomponente). Der Zeitpunkt für das Aktualisieren einer Systemkonfiguration kann nach den Erfordernissen bestimmt werden

- praktisch sofort
- zu bestimmten festgelegten Zeitpunkten (z.B. einmal pro Tag)
- beim Booten eines Rechners

cfengine

Der beschriebene Ansatz kann mit Hilfe der interpretativen Programmiersprache **cfengine** optimal umgesetzt werden. Ein cfengine-Programm beschreibt den Soll-Zustand eines oder mehrerer Rechnersysteme, festgestellte Unterschiede werden bei der interpretativen Abarbeitung des Programmes korrigiert. Eine wesentliche Stärke von cfengine besteht in der Möglichkeit, klassen-basierte Entscheidungsstrukturen im oben genannten Sinne zu formulieren. Cfengine-Sprachobjekte sind z.B. Rechner, Files, Programme, Skripten und Prozesse, entsprechende Operationen sind z.B. das Kopieren von Files oder File-Hierarchien, die Ausführung von Skripten und Programmen, das Senden von Signalen an Prozesse.

Bereitstellung und Pflege von System- und Anwendungs-Software

Im Wesentlichen basiert der Mechanismus der SW-Pflege in ToSCA auf drei Komponenten:

- Software-Repositories
- Konfigurationsfiles, die den Paket-Bestand eines Rechners definieren
- Prozeduren zur automatischen Installation bzw. Update von SW-Paketen

ToSCA stellt für jede unterstützte Systemplattform Software-Repositories zur Verfügung für

- vom Hersteller/Distributor gelieferte SW (wird nicht modifiziert)
- (verifizierte) Software-Updates
- darüber hinaus beigesteuerte SW-Pakete, die von den Verantwortlichen für die betreffenden Sachgebiete betreut werden (*contributed SW*)

Diese Repositories sind die Basis sowohl für die (Erst-)Installation von System- und Anwendungssoftware als auch für die Propagierung von SW-Updates auf die jeweiligen Rechner.

Spezielle Konfigurationsfiles legen bezogen auf die Funktionsklasse fest, welche SW-Pakete auf Rechnern dieser Funktionsklasse zu installieren sind. Die Konfigurationsfiles enthalten nur die Paketnamen. Welche konkrete Version eines Paketes installiert werden soll, legen die SW-Repositories fest. Dabei gilt der Grundsatz, dass sich von jedem SW-Paket nur die jeweils aktuelle Version in einem der Repositories befindet. Korrigierte SW-Komponenten (z.B. nach Beseitigung von Sicherheitslücken) werden in das Update-Repository abgelegt und gleichzeitig die alte Version aus dem Repository entfernt. Der Austausch der SW-Komponente auf einem Rechner erfolgt, wenn die Prozeduren zum automatischen SW-Update auf diesem Rechner ausgeführt werden. Im Regelfall passiert das einmal täglich. In analoger Weise wird die Neuinstallation eines (oder mehrerer) SW-Pakete angefordert, indem die Namen der Pakete in das Konfigurationsfile eingetragen werden. Den "Rest" erledigen wiederum die o.g. Prozeduren. Diese basieren auf Verfahren, die abhängig von der jeweiligen Betriebssystemfamilie sind (z.B. im Linux: **yum**).

Unter diesen Voraussetzungen ist es notwendig, die Aktualität und Konsistenz der SW-Repositories zu jedem Zeitpunkt aufrecht zu erhalten. Aus diesem Grund wird das Verfahren zur SW-Pflege durch Technologien für den Bau von SW-Paketen, Konventionen zur Bereitstellung von *contributed SW* sowie Policies zur Qualitätssicherung gestützt.

Datenaufzeichnung und "Real World"-Informationen

Für jedes betreute Rechnersystem werden bestimmte Daten aufgezeichnet und in sog. **LOG** -Repositories für diesen Rechner abgespeichert. Dazu gehören u.a.

- Informationen über die Hardware-Konfiguration (einschließlich Änderungs-Protokolle)
- Informationen über das Betriebssystem
- der aktuelle SW-Bestand
- Kopien rotierter Log-Files bestimmter Betriebssystem-Komponenten

- Protokolle von cfengine-Läufen

Da diese Daten im Netzwerkfilesystem liegen, sind sie zu jedem Zeitpunkt verfügbar und auswertbar für Bestandsaufnahmen, Fehlersuche usw. Entscheidend ist, dass diese Daten automatisch durch entsprechende SW-Tools erzeugt und abgespeichert werden, es handelt sich praktisch um Selbstauskünfte des Systems.

Allerdings müssen einige spezifische Daten für jeden Rechner von Hand gepflegt werden. Solche Daten bezeichnet man in ToSCA "Real World"-Informationen. Sie können nicht automatisch erfasst und geändert werden, sondern müssen von den zuständigen SysAdmins festgelegt und per Hand in eine Datenbank eingegeben werden. Das erfolgt erstmalig mit der Integration eines Rechners in die ToSCA-Technologie und betrifft Daten, die auf Entscheidungen des SysAdmins bzw. des Betreibers basieren, z.B.

- die Festlegung der **Systemplattform-Klasse**
- die Einordnung (oder Neudefinition) der **Funktionsklasse** für den Rechner
- den oder die Funktionsverantwortlichen (Loginkennzeichen)
- als Bezugsdaten: den gewählten Hostnamen (gleich **Host-Klasse**) sowie die Domäne
- Standort (Gebäude, Raum, bei Servern evtl. Rack-Stellplatz)
- Einrichtung des Besitzers/Betreibers (z.B. Fakultät, Institut, Lehrstuhl)
- Ansprechpartner vor Ort (Loginkennzeichen)

Der Pflegeaufwand ist nicht besonders hoch, selbst wenn man ins Kalkül zieht, dass es sich um eine sehr große Anzahl von Rechnersystemen handelt. Das Problem besteht allerdings darin, dass die Pflege solcher Daten von "unzuverlässigen Menschen" erfolgt, die allzu oft einfach vergessen, diese Daten zu aktualisieren. (Der Rechner selbst kann keine Auskunft darüber geben, dass sich z.B. der Ansprechpartner oder der Standort geändert haben.) Die Konzentration dieser Daten in einer Datenbank und die Buchführung über alle vorgenommenen Änderungen (CVS) erleichtern es, die Daten konsistent zu halten. Zumindest können eventuelle Inkonsistenzen durch entsprechende Prüf-Skripte angezeigt werden.

SysAdmin-Autorisierung

Wie bereits erwähnt sind an der Systemadministration mehrere Personen mit unterschiedlichen Aufgaben und Verantwortungsbereichen beteiligt. Für diese Personen und Personengruppen müssen insbesondere folgende Fragen geklärt werden

- Welche privilegierten Aktionen können von wem auf einem Rechner ausgeführt werden?
- Wer hat auf welche ToSCA-Repositories im Netzwerkfilesystem Lese- bzw. Schreiberlaubnis?

Die Grundlage für diese Entscheidungen bilden Datenbanken, in denen die verschiedenen Verantwortungsbereiche und die jeweils verantwortlichen Personen definiert sind. Daraus werden über entsprechende Skripte die Privilegien und Zugriffsrechte generiert. Dabei erfolgt eine Abbildung auf die von den Betriebssystemen bereitgestellten Mechanismen zur Ausführung privilegierter Aktionen. In Linux-Systemen steht z.B. der **sudo** -Mechanismus zur Verfügung, der über `/etc/sudoers` konfiguriert werden kann. Wie in ToSCA üblich, wird dieses Konfigurationsfile als Prototyp in den entsprechenden Repositories für die Host-Klassen erzeugt und in einem zweiten Schritt (per cfengine) auf den Rechner kopiert.

Ausblick

Die Betreuung von Rechnersystemen ist ein bewegliches Ziel: auf Grund der vielfältigen Anforderungen und der täglich neu zu lösenden Probleme muss ToSCA ständig weiter entwickelt und verbessert werden. Gegenwärtig wird ToSCA hauptsächlich für die Systemadministration von Linux-Rechnersystemen (Fedora Core, Scientific Linux, jeweils für die X86-Architektur) eingesetzt. Als eines der nächsten Projekte soll die Integration der Betriebssysteme WXP und W2003 realisiert werden. Die Erschließung weiterer Architekturen (x86_64, ia64) für Linux ist ebenso vorgesehen wie die Einbeziehung der automatischen Installationsverfahren (Kickstart, Imaging) in die ToSCA-Technologien. Aus diesen Entwicklungen sollen jeweils entsprechende ADMIN-Dienste abgeleitet werden, die von Angehörigen der TU Chemnitz in Anspruch genommen werden können. Grundsätzlich bestehen dabei zwei Möglichkeiten:

- die ADMIN-Verantwortung wird vom Auftraggeber komplett an das URZ übergeben oder
- die bereitgestellte Verfahren werden eigenverantwortlich genutzt

In die zweite Gruppe fallen die Dienste zur Rechner-Installation bzw. zum Software-Update.

Literaturhinweise

- A Toolbox for System Configuration and Administration (ToSCA)
- Cfengine: A configuration engine
- Automatisches Software-Update
- Überwachung von Diensten (Service Monitoring)
- yum: Yellow dog Updater, Modified

Matthias Clauß, Oktober 2004

Sicheres Programmieren mit PHP (Teil 3)

In den ersten beiden Ausgaben der "Mitteilungen des URZ" 2004 haben wir bereits Hinweise zur sicherheitsbewussten PHP-Programmierung gegeben. In diesem Artikel soll nun die Upload-Funktion von PHP beleuchtet werden.

An dieser Stelle möchten wir die kleine Artikelserie (nachzulesen unter <http://www.tu-chemnitz.de/urz/www/php/secure.html>) fortsetzen. Denn "Sicheres Programmieren mit PHP" ist weiterhin ein brisantes Thema. So gab es am 5.10.2004 eine Warnung vom DFN-CERT (<http://cert.uni-stuttgart.de/archive/win-sec-ssc/2004/10/msg00015.html>), in der eine massive Ausnutzung von Lücken in unsicher programmierten PHP-Skripten beschrieben wird. Und es waren auch WWW-Seiten im Campusnetz betroffen!

Auch bei diesem Angriff war das "blinde Vertrauen" in Daten von externer Quelle (hier in der HTTP-Anforderung) die Schwachstelle. Da bekanntlich Wiederholung die Mutter der Weisheit ist, stelle ich den Merksatz aus dem letzten Artikel nochmals voran:



Vertrauen Sie keinen Werten, die über Browsereingaben, den URL oder Cookies in das PHP-Skript gelangen. Alle externen Parameter, selbst wenn sie aus versteckten Feldern oder Auswahlmenüs kommen, müssen einer Plausibilitätsprüfung unterworfen werden, bevor sie im Programm verwendet werden.

Diese Tests und Überprüfungen sind mitunter aufwändig - Sicherheit hat ihren Preis! Im Folgenden wollen wir uns eine weitere, aus Sicht der Sicherheit kritische "Einfallsmöglichkeit" für externe Daten näher ansehen.

Datei-Upload

PHP bietet Funktionen, mit denen sich ziemlich einfach ein Datei-Upload (Hochladen von Dateien) vom WWW-Browser auf den WWW-Server realisieren lässt. Eine Erklärung des nötigen HTML-Formulars und der PHP-Anweisungen finden Sie in der PHP-Dokumentation (<http://www.tu-chemnitz.de/docs/php/features.file-upload.html>).

Hier folgt nur ein kritischer Ausschnitt - ein rudimentäres HTML-Formular und das Kopieren einer hochgeladenen Datei aus dem temporären Bereich in das vorgesehene Verzeichnis.

```
<form enctype="multipart/form-data" action="..." method="post">
  <input name="datei" type="file" />
  <input type="submit" value="Datei hochladen" />
</form>
```

```
<?php
$upload_verzeichnis = '/afs/tu-chemnitz.de/.../upload';
```

```

# Name für Upload-Element im Formular heißt 'datei'
if (isset($_FILES['datei']['name'])) {
    $dateiname = $_FILES['datei']['name'];
# Dateinamen prüfen: Nur Buchstaben, Punkt, Unter- und Bindestrich erlaubt:
    if (ereg('^[a-zA-Z0-9._-]*$', $dateiname)) {

# WICHTIG: Prüfen, ob Datei schon existiert, um Überschreiben zu verhindern!
        if (file_exists("$upload_verzeichnis/$dateiname")) {
            echo "Datei " . htmlspecialchars($dateiname) . " existiert schon!";
        } else {
            if (move_uploaded_file($_FILES['datei']['tmp_name'],
                "$upload_verzeichnis/$dateiname")) {

                echo "Ok";
            } else {
                echo "Fehler: " . $_FILES['userfile']['error'];
            }
        }
    } else {
        echo "Fehler: Ungültiger Dateiname " . htmlspecialchars($dateiname);
    }
}
?>

```

Trotz dieser Vorsichtsmaßnahmen bietet ein solches Verfahren natürlich ein "Einfallstor", über das auch unliebsame Dateien, etwa Schadprogramme, in unser System gelangen können. Deshalb sind gründliche Überlegungen und sorgfältige Programmierung hinsichtlich der Sicherheit erforderlich.

Bieten Sie eine solche Upload-Möglichkeit möglichst **nicht öffentlich** für jedermann an, sondern erlauben Sie das nur über eine Authentisierung für Berechtigte. Hinweise zum Zugriffsschutz über Anweisungen in der Datei **.htaccess** finden Sie unter Apache: Zugriffskontrolle (<http://www.tu-chemnitz.de/urz/www/access.html>).

Es ist besonders auf das Verzeichnis zu achten, in das die hochgeladene Datei geschrieben werden soll. Da dieses Verzeichnis für den betreffenden WWW-Server schreibbar sein muss, ist hier besondere Sorgfalt nötig:

- Verwenden Sie ein separates Verzeichnis, in dem keine eigenen Dateien stehen.
- Stellen Sie nur die unbedingt erforderlichen AFS-Rechte ein, z.B. dem WWW-Server `www-user.tu-chemnitz.de` nur das Listen und Einfügen neuer Dateien erlauben (nicht aber das Lesen oder Überschreiben):
urz:www-user li

Außerdem müssen Sie sicherstellen, dass Dateien dieses Upload-Verzeichnisses nicht direkt via WWW-Browser lesbar sind:

- Legen Sie das Verzeichnis am besten außerhalb Ihres WWW-Bereiches (**nicht** unter `/afs/tu-chemnitz.de/www/root` oder `$HOME/public_html`)
- Entfernen Sie das AFS-Leserecht für **system:anyuser** und die WWW-Server.

- Oder schützen Sie das Verzeichnis durch Anweisungen in der Datei **.htaccess**

```
# Direkten Zugriff auf alle Dateien unterbinden
order deny,allow
deny from all
```

- Wenn Sie den lesenden Zugriff auf die hochgeladenen Dateien erlauben müssen (etwa zum Austausch von Daten unter Berechtigten), müssen Sie zumindest das Ausführen von CGI- oder PHP-Skripten unterbinden. Dann schreiben Sie im **.htaccess**

```
php_flag engine off
RemoveHandler .cgi
```

Sie sehen also auch hier, dass Sicherheit ihren Preis hat - die Konfiguration ist ziemlich komplex. Deshalb beraten wir Sie gern bei der Planung Ihrer WWW-Projekte. Ein nachträgliches Ändern bestehender Projekte zur Erhöhung der Sicherheit ist dagegen meist sehr schwierig und aufwändig.

Wenn Sie eine Upload-Fähigkeit für Ihr HOME-Verzeichnis brauchen (oder für andere Verzeichnisse, für die Sie eine Schreibberechtigung haben), können Sie auf eine fertige Lösung zurückgreifen: Benutzen Sie den Web-basierten Datei-Manager WFM des Login-Servers: <https://login.tu-chemnitz.de/wfm/>

Frank Richter, Oktober 2004

"Nutzerforum des URZ" - Neue Veranstaltungsreihe

In diesem Beitrag informieren wir darüber, warum es diese neue Veranstaltungsreihe gibt sowie über die erste Veranstaltung im September. Diese hatte das Thema "MS Windows an der TU Chemnitz". Anhand einer Art Protokoll werden der Standpunkt des URZ zum sicheren Betrieb von PCs mit Windows sowie konkrete Diskussionspunkte aufgeführt.

"Mit dieser Veranstaltungsreihe "Nutzerforum" wollen wir mit Ihnen, unseren Nutzern, in "realen" Kontakt treten, über aktuelle Fragen und Probleme bezüglich der Dienste des URZ direkt informieren, Ihre Fragen beantworten und mit Ihnen diskutieren." - So haben wir das Anliegen der Veranstaltung auf der entsprechenden Web-Seite des URZ <http://www.tu-chemnitz.de/urz/forum/> kurz umrissen. Unsererseits sehen wir die Notwendigkeit dazu, weil "virtuelles oder reales Papier" den persönlichen Kontakt nicht ersetzen können.

Wir hoffen, dass Sie, unserer Nutzer, das Angebot annehmen und mit uns und den anderen Nutzern diskutieren. Wir würden uns auch freuen, wenn von Ihnen Themenvorschläge kommen. Wir werden auch auf der Web-Seite dafür eine Möglichkeit bereitstellen.

Die aktuellen monatlichen Themen werden auf der o.g. Webseite, im Veranstaltungskalender der Uni, mit Plakaten und über die Mailingliste urz-informationen bekannt gegeben.

Am Mittwoch, dem 08. September 2004, fand die erste Veranstaltung dieser neuen Reihe statt. Das Thema lautete:

Treffen für Nutzer und Betreiber von MS-Windows-Arbeitsplätzen der TU Chemnitz

Die zahlreichen mit einem Windows-Betriebssystem arbeitenden PCs an der TU sowie die immer gravierender werdenden Sicherheitsprobleme waren für das URZ die Motivation, eine Diskussion über damit im Zusammenhang stehende Probleme zu veranstalten. Die Einladung richtete sich nicht nur an TU-Mitarbeiter, die schon Dienste des URZ nutzen, sondern an alle TU-Angehörigen. Die mehr als 50 erschienenen Teilnehmer sowie Mails von weiteren potenziellen Interessenten versteht das URZ als Signal, dass ein solches Forum gewünscht ist.

Einführung

Vom Diskussionsleiter wurde der Standpunkt des URZ zum sicheren Betrieb von PCs im Campusnetz dargelegt. Eine Alternative zur konsequenten Administration eines jeden PCs gibt es nicht, denn die Verantwortung liegt beim Betreiber.

Nicht oder schlecht administrierte PCs sind oftmals die Ursache für Einbrüche in das Campusnetz und andere PCs. Administrative Tätigkeit erfordert einen recht hohen Arbeitsaufwand. Das URZ gibt Unterstützung auf verschiedenen Ebenen:

1. Aktuelle Informationen und Tipps in den "Mitteilungen des URZ" sowie auf speziellen WWW-Seiten
2. Bereitstellen bzw. Empfehlen von Software wie z.B. sophos als empfohlene und für TU-Angehörige kostenlose (auch bei privater Anwendung) Antivirensoftware
3. Vollständige Administration eines Arbeitsplatz-PCs durch das URZ im Rahmen des Administrationsdienstes Windows XP
(Dieser ist gedacht für PCs mit konstantem Aufgabenspektrum.)
4. Installation eines PCs durch das URZ, mit dem Ziel einer vollständigen und sicheren Anfangsinstallation - "Installationsdienst Windows XP"
(Empfohlen für PCs, an denen ein häufiger Softwarewechsel bzw. Softwaretests durchgeführt werden bzw. das Arbeiten mit administrator-Rechten bei speziellen Aufgaben unbedingt notwendig ist.)

Das Finden solcher Informationen wurde vorgeführt:

- Windows-Sicherheit: <http://www.tu-chemnitz.de/urz/xp/security.html>
- Computersicherheit: <http://www.tu-chemnitz.de/urz/security>
- Komplett-ADMIN-Dienst von Windows-XP-Rechnern: <http://www.tu-chemnitz.de/urz/admin/wxpadm.html>
- Installationsdienst Windows XP: <http://www.tu-chemnitz.de/urz/admin/wxpi.html>

Diskussionen

Im Rahmen der Diskussion wurden nachfolgende Themen angesprochen:

- Warum empfiehlt das URZ Windows XP statt das weniger Ressourcen "fressende" Windows 2000?
Antwort: Windows XP ist das neueste und sicherste Windows-Betriebssystem für Arbeitsplatz-PCs. Windows 2000 wird zwar noch ein paar Jahre betrieben, ist trotzdem schon abgekündigt. Windows 2000 wird vom Hersteller lediglich nachgerüstet, in einigen Komponenten.
- Könnte das URZ ein "Forum" einrichten (Austausch über Probleme und Lösungen beim Installieren und Nutzen von Windows-Software)?
Antwort: Vorschlag muss im URZ ausdiskutiert werden. Allerdings würde eine solche Liste kaum Neues bringen, gegenüber den zahlreichen schon im Internet existierenden Listen. Das URZ bietet alternativ die schon genannten Dienste an.
- Könnten Softwarelizenzen aus aufgelösten Lehrstühlen nicht im Campus weiterverwendet werden?
Antwort: Ist ein Verwaltungsproblem (Inventarisierung) und wird weitergegeben.
Diskussion: Software sollte generell inventarisiert werden, damit Lizenzen nicht "verloren gehen".
- Wäre ein Mailverteiler für Informationen über notwendige Patches (spezielle Programme zum Beheben von Sicherheitsproblemen) sinnvoll?

Antwort: Der für Windows XP empfohlene Update-Mechanismus sollte aktiviert werden, ist wesentlich schneller als Mail. Bei selbst administrierten PCs muss dies der Administrator realisieren. Bei Nutzung des Installationsdienstes ist der Update-Mechanismus konfiguriert. Im Administrationsdienst werden die notwendigen Patches automatisch integriert.

- Nach Installation des Service Pack 2 (SP2 = umfangreiche Sammlung von Programmen zur Beseitigung von Sicherheitslücken, Teil 2) ist angeblich Sophos nicht mehr aktuell?

Antwort: Dem Hersteller dieser Antivirensoftware ist das Problem bekannt und soll behoben werden.

- Im Admindienst wird eine Ergänzung des WWW-Browsers Mozilla in Form eines Plugins benötigt, was ist zu tun?

Antwort: Das Hinzufügen solcher Plugins muss behandelt werden wie die Anforderung neuer Software.

(Hinweise für die Benutzung des ADMIN-Dienst Windows XP enthält entsprechende Informationen.)

- Kann beim Installationsdienst das Image im Campusnetz bereitgestellt werden?

Antwort: Dies ist das Grundprinzip des Installationsdienstes, eine Installation soll vom PC aus initiiert werden können.

(Anmerkung: An der Wiederinstallation vom PC/Arbeitsplatz aus wird zur Zeit gearbeitet, da es mit einer neu einzusetzenden Software (ghost) technologische Probleme gibt.)

- Kann der Vorgang zur Installation zusätzlicher Drucker im Admindienst vereinfacht werden, wie auch die Festlegung des Standarddruckers?

Antwort: Ist schon vereinfacht worden; außerdem steht mittlerweile schon eine größere Anzahl von Druckerpaketen bereit. Der Standarddrucker wird auf Anforderung festgelegt.

- Aktivitäten/Empfehlungen des URZ zum Einsatz des Service Pack 2:

- Ankündigung, dass die Pools noch im September mit dem Service Pack 2 versehen werden.
- Arbeitsplatz-PCs im Rahmen des Admindienstes werden später (voraussichtlich November) aktualisiert, da weitere Komponenten von diesem SP2 tangiert werden.
- Im Installationsdienst ist der SP2 enthalten, ab Ende September.
- Beim Einsatz von SP2 wird die aktuelle OpenAFS-Version empfohlen (1.3.73 - per 19.10.2004).
- Ältere AFS-Klienten funktionieren prinzipiell auch mit SP2, aber Probleme (Cache, Boot) sind möglich.

- Eine fehlerhafte Installationsanleitung "AFS für Windows" des URZ wurde angemahnt.

- Sollte ZIN nicht von allen gefordert werden?

Antwort: Über dieses "Zertifikat Internet-Nutzung" (ZIN) wird diskutiert, ein Ergebnis ist noch nicht bekannt.

Fazit

Aus Sicht des Veranstalters ist diese erste Veranstaltung als Erfolg einzuschätzen. Den anschließenden zahlreichen Diskussionen kann Ähnliches entnommen werden. In den nachfolgenden Wochen wurde wesentlich mehr Interesse an den Diensten des URZ festgestellt, vor allem auch eine differenziertere Anforderung hinsichtlich Nutzung von Admindienst oder Installationsdienst.

Wie häufig bei solchen Veranstaltungen festzustellen, sind die Interessen der Teilnehmer sehr vielschichtig. Bei künftigen Veranstaltungen sollten speziellere, auf jeweils eine bestimmte Klientel zugeschnittene Themen gewählt werden.

Christoph Ziegler, Ursula Riedel, Oktober 2004

IP-Adressvergabe

*Aktuelle Informationen zum Umgang mit IP-Adressen in den Professuren im Zusammenhang mit der Einführung der webbasierten Managementsoftware **WebDNS**.*

Die TU Chemnitz hat vom DFN-Verein den Class-B-Adressbereich 134.109 zur Verfügung gestellt bekommen. Die Verantwortung für den Adressbereich liegt beim URZ. Der Adressbereich ist in Subnetze eingeteilt und die einzelnen Adressen werden auf Antrag vergeben. Für jede vergebene Adresse muss eine verantwortliche Person bekannt sein. Die Zuordnung von Ansprechpartnern zu IP-Adressen ist insbesondere auch deshalb wichtig, um bei Problemen (Viren und Wurmbefall, Hackerangriff, ...) zeitnah informieren und reagieren zu können.

Im September 2004 wurde eine Web-Datenbank-Schnittstelle **WebDNS** für die IP-Adressvergabe in Betrieb genommen. Die bisherige halbautomatische Pflege der DNS-Konfigurationsdateien wird damit weitgehend automatisiert. Neben der Managementschnittstelle für den **Hostmaster** wird es auch eine Webschnittstelle für die **IP-Verantwortlichen in den Professuren** geben.

Aus der Datenbank ist eine zeitnahe Übernahme der Daten ins DNS (Nameserver) und für den DHCP-Server möglich.

IP-Verantwortliche in den Professuren

Für jede Professur sollte ein verantwortlicher Mitarbeiter (URZ-Account erforderlich) für IP-Adressen benannt sein. In manchen Fakultäten macht das eine Person für mehrere Professuren. Die Person muss nicht mit dem Systemverantwortlichen oder Nutzer des Rechners übereinstimmen.

- Ansprechpartner bei Problemen
- Aktualisierung der Hostinformationen (Hardware, MAC, Betriebssystem) über ein Webinterface
- Freigabe der IP-Adresse bei Verschrottung
- Wechsel der Verantwortung bei Umsetzung des Rechners oder Verlassen der Einrichtung
- Jährliche Verlängerung der IP-Adressnutzung nach Aufforderung durch das URZ über ein Webinterface
- Neubeantragung von IP-Adressen über Formular oder Webinterface

Leistungen von WebDNS

WebDNS basiert auf den Erfahrungen der IP-Adressverwaltung der vergangenen Jahre und wurde von den Mitarbeitern des URZ Frank Richter und Jens Junghänel konzipiert und implementiert.

Leistungsumfang:

- Web-Oberfläche für alle erforderlichen Aufgaben von **Hostmaster** und **IP-Verantwortlichen in den Professuren**
 - Vergabe von IP-Adressen und Erfassen allen relevanten Informationen, wie **Hostname, Hardwareadresse, Rechner-/Gerätetyp, Betriebssystem**, etc.
 - Aktualisieren dieser Informationen bei Änderungen bzw. Löschung
 - zeitnahes Generieren der Konfigurationsdateien für DNS und DHCP - der Betrieb eigener DHCPD-Server ist nicht mehr erforderlich
 - Umfangreiche Suchfunktionen für die Generierung von Übersichtstabellen
- Datenbank **mySQL**
- skriptgesteuerte Programme für Routineaufgaben:
 - jährliche Inventur mit Aufforderung zur Verlängerung oder Rückgabe der IP-Adressen
 - Ermittlung von IP-Adressen ohne gültigen IP-Verantwortlichen
 - statistische Auswertungen

Was ändert sich?

- Verkürzung der Bearbeitungszeiten
- zeitnahes Ändern von Rechnerinformationen (insbesondere Hardwareadresse für DHCP)
- IP-Adressen werden für jeweils 1 Jahr ausgeliehen, wobei einfache Mittel zur Verlängerung bereitstehen
- die IP-Verantwortlichen sind aktuell und können somit bei Problemen kurzfristig informiert werden
- an Studenten werden in der Regel keine statischen IP-Adressen vergeben
- pro Professur oder auch für mehrere Professuren sollte es nur einen IP-Verantwortlichen geben
- IP-Adressen ohne gültigen IP-Verantwortlichen werden stillgelegt

Dynamische IP-Adressen für Gastarbeitsplätze in den Professuren

Ähnlich wie im WLAN und an Netzdosens in öffentlichen Räumen bieten wir auch für Rechnernetzanschlüsse in den Räumen der Professuren ein **dynamische IP-Adressvergabe** an. Eine Nutzung von "freien" (gerade nicht benutzten) IP-Adressen sollte unterbleiben. Im Problemfall ist kein Rückschluss auf den betroffenen Rechner möglich. Ist eine Netzdose für die **dynamische IP-Adressvergabe** konfiguriert, kann jeder, der sich als URZ-Nutzer authentifizieren kann, einen Netzzugang erhalten.

Günther Fischer, Oktober 2004

Windows XP Service Pack 2 - Erfahrungen im URZ

Von Microsoft werden in regelmäßigen Abständen Patches und Service Packs zur Behebung von Sicherheitslücken und Fehlern im Windows-Betriebssystem herausgegeben. Seit August diesen Jahres wird die finale Version des Windows XP Service Pack 2 zum Download angeboten und zur Installation empfohlen.

An neuen Funktionen hat es den Windows Firewall, Pop-up Blocker für den Internet Explorer und das neue Windows Security Center sowie kumulativ alle zu Windows XP herausgegebenen Patches zum Inhalt.

Die Anwender von AFS sollten vor der Installation des SP2 die Version des genutzten AFS-Klienten ermitteln und die zur Zeit aktuellste Version (1.3.73) installieren. Diese Version bietet den Vorteil, dass sie auf die Belange des Windows-Firewall eingeht und die erforderlichen Ports automatisch öffnet.

Diese Information wird in der Hauptsache den Windows-Firewall betrachten:

Das Service Pack 2 (SP2) für Windows XP enthält wesentliche Änderungen in der Komponente "Windows Firewall", die bisher als "Internet Connection Firewall" (ICF) bezeichnet wurde. Realisiert wird der "Windows Firewall" durch den Dienst "Windows-Firewall/Gemeinsame Benutzung der Internetverbindung" (Dienstname SharedAccess).

Der Windows Firewall blockiert den unaufgefordert eingehenden Verkehr, es sei denn, er ist als erlaubt spezifiziert. Ausgehender Verkehr (außer einigen ICMP-Nachrichten) wird hingegen nicht blockiert und kann auch nicht blockiert werden! In Windows XP SP1 war der Firewall standardmäßig nicht aktiviert (disabled) und musste explizit aktiviert und konfiguriert werden. In Windows XP SP2 hingegen ist der Firewall für alle Verbindungen (LAN, Dial-Up und VPN) aktiviert und mit einer globalen Konfiguration versehen, die für alle Verbindungen Gültigkeit hat. Außerdem können für jede Verbindung unterschiedliche Einstellungen vorgenommen werden. Diese Einstellungen können nur von Administratoren (administrator-Recht) vorgenommen werden!

Zusätzlich gibt es einen neuen Modus, der bei aktiviertem Firewall alle Ausnahmen blockt. Das kann für Laptops genutzt werden, die über unterschiedliche Medien (Intranet - Modem) das Internet nutzen. Vor Windows XP SP2 war nach dem Starten des Rechners bis zum Starten des Firewall-Dienstes der Computer ungeschützt (obwohl der Firewall aktiviert war).

Mit SP2 kann auch festgelegt werden, von welchen Source-IP-Adressen unaufgeforderter Verkehr angenommen wird (alle IP-Adressen, lokales Subnetz, nutzerdefinierte Liste). Mit SP2 kann auch erwarteter Verkehr über den Programmnamen festgelegt werden. Das war vorher nur über die Konfiguration der entsprechenden Portnummern möglich, die man herausfinden musste.

In SP2 kann auch das Kommando `netsh firewall` zum Konfigurieren benutzt werden. Die entsprechenden Subkommandos können zu einem Skript zusammengefasst und ausgeführt werden.

Über die Gruppenrichtlinien können die Firewall-Einstellungen ebenfalls festgelegt werden. Dazu existiert ein Domain- und ein Standardprofil. In großen Netzwerken sind die Computer im allgemeinen durch eine separate Firewall geschützt. Die lokale Windows-Firewall sollte trotzdem aktiviert sein, weil sie vor solchen Rechnern schützt, die spezielle Verbindungen mit dem Internet benutzen und so eventuell Viren in das Netz hineinbringen und damit die separate Firewall unwirksam machen.

Die Windows-Firewall-Standard-Einstellungen können Probleme verursachen bei der Nutzung u.a. folgender Komponenten:

- Simple Network Management Protocol (SNMP) Agent
- Windows Management Instrumentation (WMI)
- Remote Management über `netsh` oder `mmc`
- Remoteunterstützung und Remotedesktop
- File und Print Sharing
- Print Service für Unix
- eingehende Verbindungen.

Wie bisher kann eine Logdatei geschrieben werden. Der Name, der Speicherort und die maximale Größe dieser Datei kann angegeben werden. Man kann auswählen, ob nur verworfene Verbindungen oder auch erfolgreiche Verbindungen protokolliert werden sollen. Ein Protokollieren der eingehenden Pakete ist nicht möglich.

Beispiele für `netsh`-Kommandos zum Überprüfen der Konfiguration:

- `netsh firewall show config`
- `netsh firewall show state verbose=enable`

In der Antwortdatei für eine unbeaufsichtigte Installation gibt es neue Sektionen für die Windows Firewall, um die Konfiguration schon hier auf den gewünschten Stand zu bringen:

- [WindowsFirewall]
- [WindowsFirewall.profile_name] (*Domain oder Standard*)
- [WindowsFirewall.program_name] (*fügt eine Ausnahme hinzu*)
- [WindowsFirewall.service_name]
- [WindowsFirewall.portopening_name]
- [WindowsFirewall.icmpsetting_name]

Ein weiteres Verfahren zur Konfigurierung der Firewall besteht in der Verwendung der Datei `Netfw.inf`. Für Konfigurationsänderungen sind dabei folgende Sektionen von Bedeutung:

- [ICF.AddReg.DomainProfile]
- [ICF.AddReg.StandardProfile] und
- [Strings] (um Einstellungen bei den Profilen hinzuzufügen)

Die realisierten Firewall-Einstellungen finden sich alle in der Registry wieder, unter dem Schlüssel:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy

Sie lassen sich unterteilen in:

- erlaubte/blockierte Anwendungen
- erlaubte/blockierte Ports
- spezifische Einstellungen für ICMP

Die Konfiguration lässt sich u.a. über START - Systemsteuerung - Windows Firewall oder über control firewall.cpl aufrufen. Wenn die Ausführung neu installierter Programme an Firewall-Regeln scheitert, werden manchmal von diesen Programmen Popup-Fenster ausgegeben, die auf blockierte Verbindungen hinweisen.

Hier ein Beispiel, wie der Firewall konfiguriert sein kann:

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile]

"EnableFirewall"=dword:00000001

"DoNotAllowExceptions"=dword:00000000

"DisableNotifications"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\

AuthorizedApplications]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\

AuthorizedApplications\List]

"C:\\Programme\\proeWildfire2.0\\i486_nt\\nms\\nmsd.exe"=

"C:\\Programme\\proeWildfire2.0\\i486_nt\\nms\\nmsd.exe:*:Enabled:nmsd"

"C:\\Programme\\proeWildfire2.0\\i486_nt\\obj\\xtop.exe"=

"C:\\Programme\\proeWildfire2.0\\i486_nt\\obj\\xtop.exe:*:Enabled:xtop"

"C:\\Programme\\proeWildfire2.0\\i486_nt\\obj\\pro_comm_msg.exe"=

"C:\\Programme\\proeWildfire2.0\\i486_nt\\obj\\pro_comm_msg.exe:*:Enabled:pro_comm_msg"

"C:\\Programme\\AnsysInc\\v81\\CommonFiles\\TCL\\bin\\intel\\wish.exe"=

"C:\\Programme\\AnsysInc\\v81\\CommonFiles\\TCL\\bin\\intel\\wish.exe:*:Enabled:ANSYS_wish"

"C:\\Programme\\AnsysInc\\v81\\Ansys\\bin\\intel\\ansys.exe"=
"C:\\Programme\\AnsysInc\\v81\\Ansys\\bin\\intel\\ansys.exe:*:Enabled:ANSYS_exe"

"\\\\lafs\\al\\tu-chemnitz.de\\dept\\wpx\\sw\\maple_95\\bin.win\\mserver.exe"=
"\\\\lafs\\al\\tu-chem-
nitz.de\\dept\\wpx\\sw\\maple_95\\bin.win\\mserver.exe:*:Enabled:MAPLE_mserver"

"\\\\lafs\\al\\tu-chemnitz.de\\dept\\wpx\\sw\\maple_95\\jre\\bin\\java.exe"=
"\\\\lafs\\al\\tu-chem-
nitz.de\\dept\\wpx\\sw\\maple_95\\jre\\bin\\java.exe:*:Enabled:MAPLE_java"

"C:\\Programme\\Symantec\\Ghost\\ngctw32.exe"= "C:\\Programme\\Syman-
tec\\Ghost\\ngctw32.exe:134.109.0.0/255.255.0.0:Enabled:GhostClient"

"C:\\WINDOWS\\system32\\sessmgr.exe"="C:\\WINDOWS\\system32\\sessmgr.exe:*:Disabled:@xpsp2res.dll,-22019"

[HKEY_LOCAL_MACHINE\\SYSTEM\\CurrentControlSet\\Services\\SharedAc-
cess\\Parameters\\FirewallPolicy\\
StandardProfile\\GloballyOpenPorts]

[HKEY_LOCAL_MACHINE\\SYSTEM\\CurrentControlSet\\Services\\SharedAc-
cess\\Parameters\\FirewallPolicy\\
StandardProfile\\GloballyOpenPorts\\List]

"3389:TCP"="3389:TCP:134.109.200.0/255.255.254.0:Enabled:@xpsp2res.dll,-22009"

"7001:UDP"="7001:UDP:*:Enabled:AFS CacheManager Callback (UDP)"

"7001:TCP"="7001:TCP:*:Enabled:AFS CacheManager Callback (TCP)"

"139:TCP"="139:TCP:134.109.0.0/255.255.0.0:Enabled:@xpsp2res.dll,-22004"

"445:TCP"="445:TCP:LocalSubNet:Disabled:@xpsp2res.dll,-22005"

"137:UDP"="137:UDP:LocalSubNet:Disabled:@xpsp2res.dll,-22001"

"138:UDP"="138:UDP:LocalSubNet:Disabled:@xpsp2res.dll,-22002"

"5900:TCP"="5900:TCP:134.109.176.0/255.255.254.0,134.109.200.0/255.255.254.0:Enabled:WinVNC"

"1346:UDP"="1346:UDP:134.109.200.0/255.255.254.0:Enabled:GhostConsole"

[HKEY_LOCAL_MACHINE\\SYSTEM\\CurrentControlSet\\Services\\SharedAc-
cess\\Parameters\\FirewallPolicy\\
StandardProfile\\IcmpSettings]

"AllowInboundEchoRequest"=dword:00000001

Empfehlungen seitens des URZ: siehe WWW-Veröffentlichung bzw. "Mitteilungen
des URZ" 3/2004

Verweise/Links auf andere Informationsquellen: [http://www.micro-
soft.com/windowsxp/sp2/topten.mspx](http://www.microsoft.com/windowsxp/sp2/topten.mspx)

Karl-Heinz Arnold, Oktober 2004

Adobe-Rahmenvertrag

Wie vielleicht bekannt ist, bot ein Rahmenvertrag mit der Firma Adobe (und einem entsprechenden Softwarehändler) seit längerer Zeit die Möglichkeit, die Adobe-Software sehr kostengünstig innerhalb der TU Chemnitz einzusetzen. Da Adobe Marktführer bei der PDF-Technologie ist, haben diese Produkte bei uns - genauso wie an allen anderen Hochschulen - eine große Verbreitung gefunden.

Im Juli diesen Jahres hat Adobe - für alle überraschend - die Bedingungen des entsprechenden Lizenzprogramms bundesweit drastisch geändert (Bezugsmöglichkeiten, Preise), was de facto einer Kündigung der bisherigen Verfahrensweise entsprach. Die Bereitstellung von kostengünstigen Adobe-Lizenzen innerhalb der TU Chemnitz war deshalb zunächst blockiert.

Da alle Hochschulen von dieser Situation betroffen waren, hat der Arbeitskreis Softwarelizenzen im ZKI (Zentren für Kommunikation und Informationsverarbeitung in Lehre und Forschung, einem Zusammenschluss aller Hochschulrechenzentren) Verhandlungen mit Adobe aufgenommen. Diese gestalteten sich sehr schwierig und zäh, führten aber letztlich zum Erfolg: es gibt jetzt bundesweit genau einen Rahmenvertrag mit der blumigen Bezeichnung "Adobe Open Options, Mitgliedsvertrag zum Vertragslizenzprogramm für Bildungseinrichtungen". Das Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften hat diesen Vertrag mit Adobe abgeschlossen und alle interessierten Hochschulen können ihm "beitreten". Für die TU Chemnitz ist das in Vorbereitung und sollte zum Zeitpunkt der Veröffentlichung dieser Zeilen erfolgt sein.

Damit gelten nun folgende Bedingungen:

- bezugsberechtigt für Adobe-Produkte sind alle Angehörigen der TU Chemnitz und der An-Institute
- die Software darf nur für dienstliche Zwecke (Lehre, Forschung, Verwaltung) auf Computern der Einrichtung benutzt werden
- entsprechend dem Endnutzer-Lizenzvertrag bei Adobe (EULA) ist Home-Use möglich, eine (dienstliche) Lizenz darf also auch zu Hause oder auf einem Laptop verwendet werden, sofern nicht zwei Personen gleichzeitig die Software verwenden
- Software ist verfügbar für Windows, Mac und UNIX (hier nur FrameMaker)
- die Kosten sind ähnlich günstig wie das unter den alten Vertragsbedingungen war (z.B. knapp 20 € für Acrobat)
- Lizenzen (ggf. als Software auf CD) und Dokumentationen können beim URZ angefordert werden
- dafür sind notwendig: eine ausgefüllte Überlassungsvereinbarung (Online-Formular: <http://www.tu-chemnitz.de/urz/anwendungen/form/ueberlassung-ow.php>) und ein unterschriebener Materialentnahme-Schein
- der Besteller bekommt das Bestellte per Hauspost zugestellt
- die innerbetriebliche Umbuchung des Entgelts erfolgt zum Anfang des Folgemo-

nats - dabei sind die zum Zeitpunkt der Lizenzabrechnung durch das URZ beim Lieferanten gültigen Preise relevant, gegenüber der von uns im Intranet veröffentlichten Liste (<https://www.tu-chemnitz.de/urz/anwendungen/preise/adobe.html>) sind geringe Modifikationen möglich.

Alle Informationen zum Bezug von Adobe-Software sind unter <http://www.tu-chemnitz.de/urz/anwendungen/standard/adobe.html> zu finden.

Ansprechpartner: Edwin Wegener

Gruppe Anwendungen, Oktober 2004

Kurzinformationen

Umstellung auf Kerberos Version 5

Wie in der letzten Ausgabe angekündigt, wurde am letzten Wochenende im August die Umstellung unserer Authentisierungsserver vom OpenAFS kaserver auf Heimdal Kerberos 5 durchgeführt. Damit waren auch einige Umstellungen auf der Seite der Clients verbunden (insbesondere in Systemen, die vom URZ betreut werden).

Die jetzt betriebenen Server verstehen neben Kerberos 5 auch die Protokolle Kerberos 4 und die zu AFS gehörenden Authentisierungsprogramme (`klog`) und -moduln (PAM), so dass die weitere Umstellung von einzelnen Diensten schrittweise vorangetrieben werden kann.

Einzelheiten zur Benutzung und Konfiguration von selbstverwalteten Systemen werden wir auf der Seite Kerberos an der TU Chemnitz - <http://www.tu-chemnitz.de/urz/kerberos/> veröffentlichen.

Ansprechpartner: Thomas Müller

Gruppe System, Oktober 2004

Software-News

CFX und ICEM

CFX ist ein Finite-Volumen CFD-Programmsystem insbesondere zur Lösung der Navier-Stokes-Gleichungen. Es arbeitet mit unstrukturierten, hybriden Rechengittern, in denen geometrische Elemente verschiedener Formen in beliebiger Anordnung vorkommen können. Durch die flexible Gittergenerierung ist eine nahezu automatische Vernetzung von komplexen Geometrien möglich.

Die aktuelle Version CFX-5 bietet ein großes Spektrum von Anwendungsmöglichkeiten wie z.B.*):

- Reibungsbehaftete laminare und turbulente Strömungen
- Kompressible und inkompressible Strömungen
- Sehr leistungsfähige Turbulenzmodelle (z.B. SST-Modell) und neuartige Methoden zur Wandbehandlung für zuverlässige Berechnung der Wandreibung (Widerstandskoeffizienten, Wirkungsgrade) und des Wärmeübergangs
- Wärmeleitung im Fluid und in Festkörpern, Wärmeübergang
- Mehrphasenströmungen (Euler-Euler-Modell, Lagrange'sche Partikel, Verdampfung)
- Freie Oberflächen

- Stehende und rotierende Bezugssysteme für z.B. Turbomaschinen-, Pumpen- und Lüfterberechnungen
- Verbrennungs- und Strahlungsmodelle, reagierende Strömungen

ICEM ist ein leistungsfähiger Postprozessor zur Gittergenerierung und bildet somit eine wesentliche Voraussetzung zur effektiven Nutzung von CFX.

Im September/Oktober 2004 wurde je eine Lizenz von CFX-5 und ICEM beschafft, die über zentrale Lizenzmanager im URZ verwaltet werden. Die Finanzierung erfolgte unter wesentlicher Beteiligung der Fakultät für Maschinenbau und der dortigen Professur Technische Thermodynamik. Dieser Bereich ist auch der Hauptnutzer der Software, sowohl für Forschungszwecke als auch zunehmend für die studentische Ausbildung. Ansprechpartner innerhalb der Professur ist Dr. Urbaneck (thorsten.urbaneck@mb.tu-chemnitz.de). Die Softwareprodukte CFX und ICEM können prinzipiell auch von anderen TU-Angehörigen genutzt werden, dabei ist eine Kostenbeteiligung erstrebenswert. Interessenten melden sich bitte bei Dr. Urbaneck oder beim Autor des Artikels.

Informationen zu CFX im URZ: <http://www.tu-chemnitz.de/urz/anwendungen/cfx/>.

Anbieter der genannten Produkte ist die Firma ANSYS Germany GmbH: <http://www.cfx-germany.com/>.

*) übernommen von <http://www.cfx-germany.com/cfx5.html>

Ansprechpartner im URZ: Dr. Wolfgang Riedel

CAD-Software

Zeitgleich mit dem Systemupgrade der URZ-Pools auf MS Windows XP konnten auch die wichtigsten CAD-Angebote aktualisiert werden.

Dazu gehören in erster Linie die Autodesk-Produkte. Unter Windows XP ist jetzt eine 20-er Netzwerklizenz für diese Applikationen installiert. Sie beinhaltet die folgenden Komponenten:

- AutoCAD 2004
- Mechanical Desktop 2004
- Inventor 7

Hiermit sind jetzt die Unverträglichkeiten älterer Autodesk-Produkte mit Windows XP beseitigt.

Desweiteren gibt es neue Versionen der PTC-Software. Unter Windows XP sind dies:

- Pro/ENGINEER Wildfire 2.0
- Pro/Mechanica Wildfire 2.0

Unter Linux steht in den URZ-Pools (außer Phil.-Pool RH 41, Raum 338) ebenfalls die aktuelle Version Pro/ENGINEER Wildfire 2.0 zur Verfügung.

Pro/ENGINEER Wildfire 2.0 bietet vor allem Neuerungen in der 3D-Zeichnungs-Technologie und eine verbesserte Produktivität von NC-Prozessen. Fertigungsrelevante Zusatzinformationen können jetzt direkt in der 3D-Konstruktion an den 3D-Geometrieobjekten platziert werden.

Auch weiterhin können sämtliche CAD-Softwareprodukte in den URZ-Pools von den Mitarbeitern und Studenten der TU Chemnitz kostenfrei genutzt werden. Informationen zu CAD-Software im URZ: <http://www.tu-chemnitz.de/urz/anwendungen/cad/>

Ansprechpartner: Dagmar Dippmann

S-Plus

Seit dem 15.10.2004 steht das Statistikprogramm S-Plus Version 6.2 unter Linux/Fedora Core 1 mit einer Netzwerklizenz zur Verfügung.

Was ist daran neu:

- Native Schnittstellen zu den Datenbanken Sybase, Oracle und IBM DB2
- Neues Interface zum Starten und Kontrollieren von S-Plus Script Batchprozessen
- Neues Reportsystem auf Basis von XML

Die S-Plus Graphlets Technologie ist erweitert worden und SAS 9 Dateien können importiert und exportiert werden. Weitere neue Funktionen und statistische Bibliotheken wurden integriert bzw. aktualisiert.

Informationen zu S-Plus im URZ: <http://www.tu-chemnitz.de/urz/anwendungen/stat/splus.html>

Ansprechpartner: Edwin Wegener

Gruppe Anwendungen, Oktober 2004

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 unseren Nutzern ein schönes Weihnachtsfest



Foto: "Chemnitz, Schloßberg", C. Ziegler

sowie Gesundheit, Glück und Erfolg im Neuen Jahr!

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: 22.10.2004

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.