



**Relay-Sperre des
GWDDG-Mailers**

Instant-Grid

**Neuer Gastzugang
im GÖNET**

GWDDG Nachrichten

9 / 2006

Inhaltsverzeichnis

| | | |
|----|---|----|
| 1. | Relay-Sperre des GWDG-Mailers | 3 |
| 2. | Kontingenzuweisung für das vierte Quartal 2006 | 4 |
| 3. | Instant-Grid: Demonstration, Entwicklung und Test von Grid-Anwendungen .. | 5 |
| 4. | Der neue Gastzugang im GÖNET | 13 |
| 5. | Kurse des Rechenzentrums | 17 |
| 6. | Betriebsstatistik August 2006 | 21 |
| 7. | Autoren dieser Ausgabe | 22 |

GWDG-Nachrichten für die Benutzer des Rechenzentrums

ISSN 0940-4686

29. Jahrgang, Ausgabe 9 / 2006

<http://www.gwdg.de/GWDG-Nachrichten>

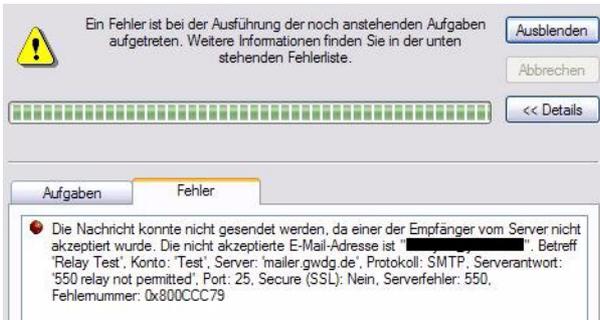
Herausgeber: Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen
Am Fassberg, 37077 Göttingen-Nikolausberg

Redaktion und
Herstellung: Dr. Thomas Otto Tel.: 0551 201-1828, E-Mail: Thomas.Otto@gwdg.de

1. Relay-Sperre des GWDG-Mailers

1.1 Einführung

Jeder, der schon einmal von einem fremden Provider kommend über den Mailserver der GWDG Mails verschicken wollte, kennt die Fehlermeldung: *550 relay not permitted*, wie sie hier unten am Beispiel von Outlook Express zu sehen ist:



Was sich dahinter verbirgt, ist das Verhalten des Mailservers der GWDG *mailer.gwdg.de*, für Mails nicht automatisch als Mail-Verteiler (Mail-Relay) zu fungieren, falls weder die Absender- noch die Empfängeradresse aus dem GWDG- bzw. Universitäts-Bereich kommen. Damit versucht man, den Missbrauch durch Spam-Versender abzuwenden, da diese sich gerne fremder Mailserver bedienen, um so weniger leicht entdeckt werden zu können.

Nun setzen inzwischen viele Nutzer Breitbandnetze wie DSL ein und kommen damit zwangsläufig von GWDG-fremden Providern. Solange die Mails an GWDG-Adressen gerichtet sind, entsteht noch kein Problem; erst wenn der Adressat außerhalb der GWDG bzw. der Universität Göttingen liegt, schlägt die Relay-Sperre unbarmherzig zu.

Die Umgehung dieses Problems ist jedoch gar nicht so schwer und führt uns zur Konfiguration der jeweiligen verwendeten Mailprogramme, denn solange man die Webmail-Interfaces wie **Squirrelmail** oder **Outlook Web Access (OWA)** nutzt, befindet man sich als Absender ja lokal auf dem Mailserver und ist von der Relay-Sperre nicht betroffen. Der GWDG-Mailer muss also nur „wissen“, dass der Nutzer berechtigt ist, ihn als Mailverteiler zu nutzen, und das geschieht natürlich am einfachsten dadurch, dass sich der Versender beim Versand authentifiziert, d. h. die GWDG-Benutzerkennung (*Userid*) und das dazugehörige Passwort angibt. Die gängigsten Mailprogramme – im Folgenden exemplarisch **Outlook Express**, **Mozilla Thunderbird** und **Office Outlook 2003** – sehen hierfür eine entsprechende Konfiguration vor.

Wichtig ist zuerst allerdings die Wahl der richtigen Serveradressen. Bei der Konfiguration eines POP3-

bzw. IMAP-Mailkontos gelten für die GWDG-Nutzer immer die folgenden Server:

Posteingangsserver:

mailbox.gwdg.de

exchange.gwdg.de (Exchange-Server)

Hierbei ist zu beachten, dass die GWDG seit Oktober 2005 mit dem Exchange-Server einen zweiten Mailserver betreibt (siehe GWDG-Nachrichten 10/2005). Alle seitdem eingerichteten Nutzer haben automatisch auf diesem ihr Konto, es sei denn, sie haben bei der Beantragung der Benutzerkennung ausdrücklich gewünscht, dass ihre Mailbox auf dem UNIX-Mailer liegen soll.

Für den Mailversand hingegen gilt für beide Mailserver generell die folgende Adresse:

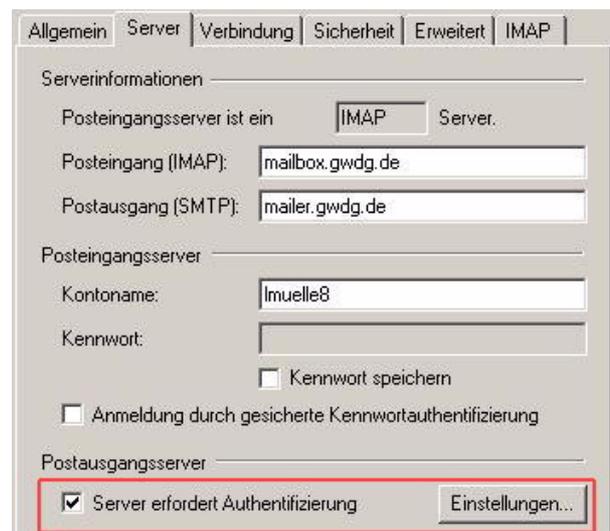
Postausgangsserver (SMTP):

mailer.gwdg.de

Um die Relay-Sperre zu überwinden, ist weiterhin zu beachten, dass der SMTP-Versand über SSL/TLS verschlüsselt erfolgt und vor allem die Senderauthentifizierung eingestellt wird, damit der Mailserver die Berechtigung entsprechend überprüfen kann.

1.2 Outlook Express

Hier erfolgt die Konfiguration im Menü „**Extras > Konten > E-Mail**“, die Wahl des entsprechenden Kontos und dann über die Schaltfläche „**Eigenschaften**“. Im Registermenü „**Server**“ muss die Authentifizierung am Postausgangsserver aktiviert werden.



Über die Schaltfläche „**Einstellungen...**“ können dann die gleichen Einstellungen wie für den

Posteingangsserver verwendet werden, da man i. d. R. über die gleiche Userid versendet wie empfängt. Im Registermenü „**Erweitert**“ wird dann – so weit noch nicht geschehen – die sichere Verbindung (SSL) aktiviert.

1.3 Mozilla Thunderbird

Hier erfolgt die Konfiguration im Menü „**Extras > Konten**“ und dort in der Rubrik „**Postausgang-Server (SMTP)**“. Als Server wird ebenfalls *mailer.gwdg.de* gewählt und die Authentifizierung mittels Benutzername und Passwort vorgenommen. Schließlich sollte auch hier noch die Verschlüsselung (TLS, wenn möglich) aktiviert sein:



1.4 Office Outlook 2003

Sofern in Outlook 2003 ein IMAP-Konto eingerichtet wird, muss im Menü „**Extras > E-Mail-Konten**“ im betreffenden Konto über die Schaltfläche „**Erweiterte Einstellungen**“ die entsprechende Konfiguration vorgenommen werden. Im Registermenü

„**Postausgangsserver**“ wird wieder die erforderliche Authentifizierung aktiviert, wobei auch hier die gleiche Einstellung wie für den Posteingangsserver gewählt werden kann:



Die Einstellung der sicheren Verbindung (SSL) erfolgt dann im Registermenü „**Erweitert**“.

Falls Outlook 2003 in Verbindung mit dem Exchange-Server eingesetzt wird, bietet sich die Methode „**RPC über HTTPS**“ an, bei der die Daten durch eine verschlüsselte HTTP-Verbindung direkt zum Exchange-Server getunnelt werden und damit auch keinerlei Probleme mit eventuell dazwischengeschalteten Firewalls wie auch der Relay-Sperre des Mailservers entstehen. Voraussetzung für diese praktische Anbindung ist Outlook 2003 und als Betriebssystem Windows XP oder Windows 2003. Wie hier die Konfiguration von Outlook 2003 vorgenommen werden muss, entnimmt man am besten der entsprechenden Webseite:

<http://www.gwdg.de/service/netze/mailer/exchange/o12003-rpc.html>

Soweit man sich an die eben beschriebenen Konfigurationshinweise hält, sollte einem reibungslosen Mailversand über den GWDG-Mailserver auch aus Fremdnetzen nichts mehr im Wege stehen.

Reimann

2. Kontingenzuweisung für das vierte Quartal 2006

Die nächste Zuweisung von Institutskontingenten für die Inanspruchnahme von Leistungen der GWDG erfolgt am Montag, den 02. Oktober 2006. Die Höhe der Kontingente wird den Instituten per Brief oder per E-Mail mitgeteilt. Die Bemessung der Institutskontingente erfolgte nach den Vorläufigen Richtlinien des Beirats der GWDG und den Ergänzungen der Beiratskommission für die Verteilung von Rechenleistung entsprechend dem Verbrauch im Zeitraum vom 01.03.2006 bis 31.08.2006. Nicht verbrauchte Kontingente werden zu 50 % in das

nächste Quartal übertragen. Negative Verbrauchswerte werden zu 100 % mit dem neuen Institutskontingent verrechnet.

Jeder Benutzer kann den aktuellen Stand des Institutskontingents durch die Eingabe des Kommandos

`kontingent`

auf einer Workstation des UNIX-Clusters oder im WWW unter dem URL

<http://www.gwdg.de/service/nutzung/kontingentierung>

abfragen. Dort besteht auch die Möglichkeit, Informationen über den Stand des separaten Druckkontingents abzurufen.

Falls in Ausnahmefällen das Institutskontingent nicht ausreichen sollte, können schriftlich begründete Anträge an die Beiratskommission für die Verteilung von Rechenleistung gestellt werden. Solche Anträge sollen bis zum 23.11.2006 im Rechenzentrum eingereicht werden; Vordrucke und Hinweise dazu sind sowohl bei der Information als auch im WWW unter dem URL

<http://www.gwdg.de/service/nutzung/antragsformulare>

erhältlich. Da aber die Bearbeitung der Anträge mittlerweile **vollständig elektronisch** erfolgt, ist die Übersendung der Anträge mit Begründung per E-Mail an die Adressen sgreber@gwdg.de oder wgriege@gwdg.de **erwünscht**.

Greber

3. Instant-Grid: Demonstration, Entwicklung und Test von Grid-Anwendungen

(Hinweis: Dieser Artikel wurde in der Zeitschrift „PIK - Praxis der Informationsverarbeitung und Kommunikation“, Heft 3/2006 (29. Jg.), S. 171 - 177, veröffentlicht!)

Zusammenfassung

Eines der Ziele von eScience- und D-Grid-Initiative ist es, innovative Infrastrukturen für verteiltes, kooperatives wissenschaftliches Arbeiten auf der Basis von Grid-Technologien zu entwickeln und deren weit verbreiteten Einsatz zu fördern. Will man dieses Ziel kurzfristig erreichen, muss ein Werkzeug zur Verfügung stehen, das auf möglichst einfache Weise den Nutzen von Grid-Technologien demonstriert und die Verwendung einer gemeinsamen unterliegenden Grid-Plattform über alle Wissenschaftsdisziplinen und alle virtuellen Organisationen hinweg erlaubt. Das Projekt Instant-Grid hat ein derartiges Werkzeug entwickelt: mit Hilfe der Instant-Grid Live-CD können Rechner in einem lokalen Netz neu gestartet und automatisch als Teile eines lokalen Grids konfiguriert werden. Einmal gestartet, ist die Instant-Grid-Funktionalität sofort über das Web-Portal verfügbar. Die Beispiel-Applikationen sind so ausgewählt, dass sie auch für Nicht-Experten verständlich sind und die Vorteile von Grids überzeugend demonstrieren.

3.1 Einführung

Grid-Technologien [1] haben sich zu einem viel versprechenden Ansatz für die Integration der Informationsverarbeitung in Industrie, Forschung und Lehre entwickelt. Aus diesem Grund hat das deutsche Bundesministerium für Bildung und Forschung die eScience-Initiative [2] gestartet, deren primäres Ziel die Einführung neuer Kooperationsformen in Forschung und Lehre ist. Eine innovative Infrastruktur für verteiltes, kooperatives wissenschaftliches Arbeiten über Kommunikationsnetze und eine effiziente Informationsversorgung sollen die Attraktivität

der Forschung im internationalen Vergleich ausbauen. Ziel ist es, den Wissensaustausch für Ausbildung und Forschung in seiner Rolle als treibende Kraft für Innovationen durch Entwicklung von offener Vernetzung mit hoher Leistung zu optimieren. Diese Vernetzung muss nahtlosen, offenen und sicheren Zugang zu wissenschaftlicher Information und Infrastruktur gewährleisten.

Im Rahmen der D-Grid-Initiative [3] soll nicht in Spezialentwicklungen für einzelne Wissenschaftsdisziplinen investiert werden, sondern in einen Satz gemeinsamer Module, die es erlauben, unterschiedliche eScience-Anwendungen und Disziplinen auf einer gemeinsamen Infrastruktur zu integrieren. Weiterhin soll schnell ein sichtbarer Mehrwert für die Anwender erzeugt werden, anstatt langwierig vorab zu standardisieren. Es muss damit kurzfristig ein Werkzeug entwickelt werden, das die weit verbreitete Nutzung einer gemeinsamen unterliegenden Grid-Plattform über alle Wissenschaftsdisziplinen und alle virtuellen Organisationen hinweg unterstützt bzw. möglich macht. Der kurzfristige Erfolg der Initiative wird entscheidend davon abhängen, wie einfach die Nutzung der verschiedenen virtuellen Ressourcen für die Wissenschaft sein wird.

In einem ersten Schritt wird es wichtig sein, die neuen Möglichkeiten und Vorteile von Grids bekannt zu machen und ihre Verwendung neuen potentiellen Nutzern und Wissenschaftsdisziplinen zu demonstrieren. Will man sich erstmalig mit Grid-Applikationen befassen, hat man zwei wesentliche Hindernisse zu überwinden: die Komplexität der Grid-Middleware, die für die nahtlose Nutzung der virtualisierten Ressourcen notwendig ist, und den derzeitigen Mangel an Grid-fähigen Applikationen, die dem neuen Nutzer die Vorteile von Grids überzeugend darstellen. Das Projekt Instant-Grid (<http://www.instant-grid.org>) zielt darauf ab, genau diese beiden Hindernisse aus dem Weg zu

räumen: es stellt eine sofort verwendbare Grid-Umgebung bereit, auf der vorkonfigurierte Grid-Applikationen als Demonstratoren für die Verwendung von Grids gestartet werden können.

Mit Hilfe der Instant-Grid Live-CD können Rechner in einem lokalen Netz neu gestartet und automatisch als Teile eines lokalen Grids konfiguriert werden. Dabei ist keinerlei Wissen über die Konfigurationsschritte notwendig, die ablaufen müssen, um das lokale Grid funktionsfähig zu machen. In den meisten Fällen erfolgt die Konfiguration des Boot Servers, der Rechenknoten, der Netzverbindungen, der Grid-Middleware und der Benutzerschnittstelle (Web-Portal) ohne jeglichen manuellen Eingriff. Einmal gestartet, ist die Instant-Grid-Funktionalität sofort über das Web-Portal verfügbar. Das Portal enthält Schnittstellen zum Start der Applikationen. Die Applikationen sind so ausgewählt, dass sie auch für Nicht-Experten der jeweiligen Gebiete verständlich sind. Sie demonstrieren überzeugend die Vorteile von Grids, u. a. auch durch die integrierte Funktionalität zur Darstellung und Überwachung der Nutzung der einzelnen Ressourcen.

Im folgenden Abschnitt wird ein Überblick über die verwendeten Mechanismen zur automatisierten Konfiguration der Hardware und der automatisierten Verteilung und Konfiguration der Grid-Middleware gegeben. Die endgültige Version des Instant-Grid wird Applikationen enthalten, die den Nutzen von Grids für rechenintensive Anwendungen, als verteilte Informationsablage und als Werkzeug für verteilte Kollaboration und virtuelle Labors demonstrieren. In Abschnitt 3 beschreiben wir die Adaption von POV-Ray als Beispiel-Applikation für Instant-Grid. Abschnitt 4 enthält Zusammenfassung und Ausblick.

3.2 Funktionsweise der Instant-Grid-CD

3.2.1 Start des Instant-Grids

Instant-Grid basiert auf einer modifizierten Knoppix-Live-CD [4], mit deren Hilfe ein PC, der so genannte Frontend, mit GNU/Linux als Betriebssystem gestartet wird. Der Vorteil einer Live-CD ist, dass sich nach Entfernen der CD und einem Neustart das System wieder in seinem ursprünglichen Zustand befindet. Nach Start des Frontends können weitere PCs im gleichen lokalen Netzwerk das Betriebssystem von dort übernehmen und sich so in Instant-Grid eingliedern. Dies geschieht mit Hilfe eines auf dem PXE-Boot-Standard basierenden Mechanismus, der in ähnlicher Weise auch im Original-Knop-

pix und in Projekten, die Live-CDs zum Aufsetzen von Clustern verwenden, benutzt wird. Dabei fungiert der von CD gestartete PC im lokalen Netzwerk als DHCP-, TFTP- und NFS-Server und ermöglicht es so, weitere Rechner im gleichen Subnetz von ihrer Netzwerkkarte zu starten und die CD per NFS als Hauptverzeichnis ihres Dateisystems zu verwenden. Sie können dann ohne Verwendung ihrer lokalen Massenspeicher als Klienten arbeiten (s. Abb. 1).

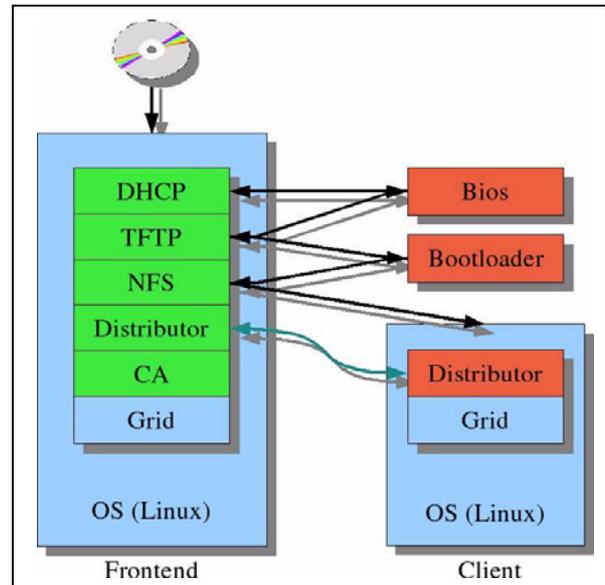


Abb. 1: Schematische Darstellung des Startvorgangs der Klienten

Unser Hauptziel bei der Implementierung dieses Mechanismus ist, ihn so zu gestalten, dass er sich ohne administrativen Eingriff in typischen Netzwerkkumgebungen verwenden lässt. Ein solcher Eingriff ist bei allen uns bekannten bisherigen Implementierungen erforderlich. Zu den automatisch zu erledigenden Aufgaben gehört die Auswahl einer geeigneten Netzwerkschnittstelle sowohl auf dem Frontend als auch auf den Klienten. Dabei müssen insbesondere eventuell bereits vorhandene DHCP-Server ermittelt werden, da hiermit ausgestattete Netzwerke sich nicht als internes Instant-Grid-Netzwerk eignen.

Nach Abschluss des Startvorgangs präsentiert sich Instant-Grid dem Benutzer über die zur Verfügung gestellten Web-Schnittstellen, die ihrerseits auf die Instant-Grid-Infrastruktur und die vorkonfigurierten Globus-Toolkit-Komponenten [5] zurückgreifen (s. Abb. 2). Letztere können auch direkt von der Kommandozeile aus verwendet werden. Eine

detailliertere Beschreibung der Komponenten findet sich in den folgenden Abschnitten.

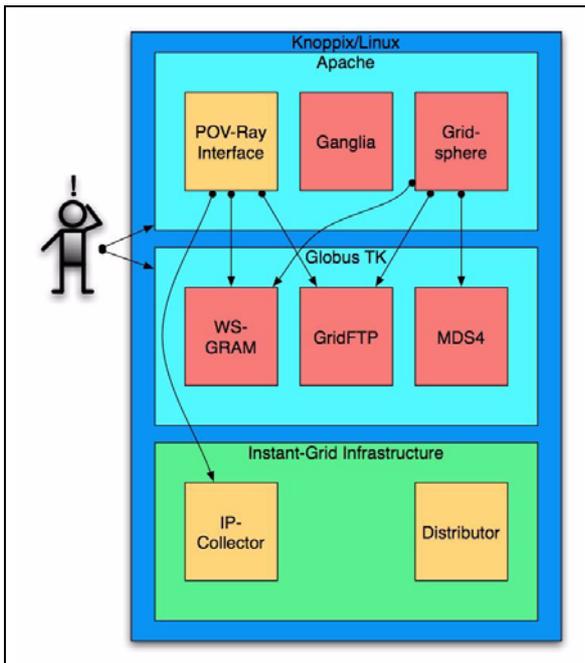


Abb. 2: Wichtige Instant-Grid-Komponenten

3.2.2 Dynamische Ressourcen-Verwaltung

Die Ressourcen in einem Grid werden, im Unterschied zu vielen Cluster-Lösungen, üblicherweise als dynamisch angesehen. Auch in Instant-Grid ist vorgesehen, dass Klienten während dessen gesamter Lebensdauer, also solange der Frontend läuft, hinzukommen oder unerreichbar werden können. Da die Topologie des Netzwerkes sowohl auf dem Frontend als auch auf den Klienten bekannt sein muss, wird ein Mechanismus benötigt, mit dessen Hilfe die Netzwerktopologie ermittelt und verteilt werden kann.

In Instant-Grid wird dazu vom Frontend aus das lokale Instant-Grid-Netzwerk nach verfügbaren Klienten durchsucht (durch die IP-Collector-Komponente) und die Konfigurationsdateien werden aktualisiert und auf ein mittels NFS exportiertes Dateisystem kopiert (durch die Server-seitige Distributor-Komponente). Dieses Dateisystem wird auf den

Klienten periodisch untersucht, und aktualisierte Konfigurationsdateien werden gegebenenfalls übernommen (durch die klientenseitige Distributor-Komponente). Auf diese Weise werden Änderungen im Instant-Grid innerhalb einer Minute auf allen Klienten bekannt.

3.2.3 Daten-Management

In Instant-Grid sind Modifikationen an den lokalen Massenspeichern normalerweise unnötig und nur nach expliziter Freigabe möglich. Für eigene Applikationen und Daten kann optional ein Verzeichnis auf einer lokalen Speicherressource des Frontends eingerichtet werden, welches dann automatisch per NFS an die Klienten exportiert und von diesen genutzt wird.

Zusätzlich zu diesem gemeinsamen Dateisystem stehen in Instant-Grid auch die Daten-Management-Dienste von Globus Toolkit zur Verfügung. Der Basisdienst ist GridFTP [6], mit dessen Hilfe Dateien zwischen den Rechnern kopiert werden können. Auf GridFTP setzt der Dienst RFT [7] (Reliable File Transfer) auf, der Daten-Transfers zusätzlich in einer SQL-Datenbank speichert. Auf diese Weise kann der korrekte Abschluss von Transfers gewährleistet werden.

3.2.4 Portal

Instant-Grid bietet als Benutzerschnittstelle zur Grid-Middleware ein Web-Portal an, das auf dem Frontend betrieben wird. Nach dem Start von Instant-Grid erscheint automatisch die Hauptseite des Portals auf dem Frontend.

Basis und Rahmen für das Instant-Grid-Portal bildet das Open-Source-Projekt Gridsphere [8]. Gridsphere ist eine Portallösung, die auf Portlets aufsetzt, die dem JSR-168-Standard entsprechen. Das Projekt besitzt eine große und rege Benutzer-gemeinde und erlaubt Entwicklern, als eines der Schlüsselemente des Projektes, die Nutzung von Portlet-Web-Applikationen, die aus dem Third-Party-Bereich stammen. Diese können dann innerhalb des Gridsphere-Portlet-Container administriert und gestartet werden.

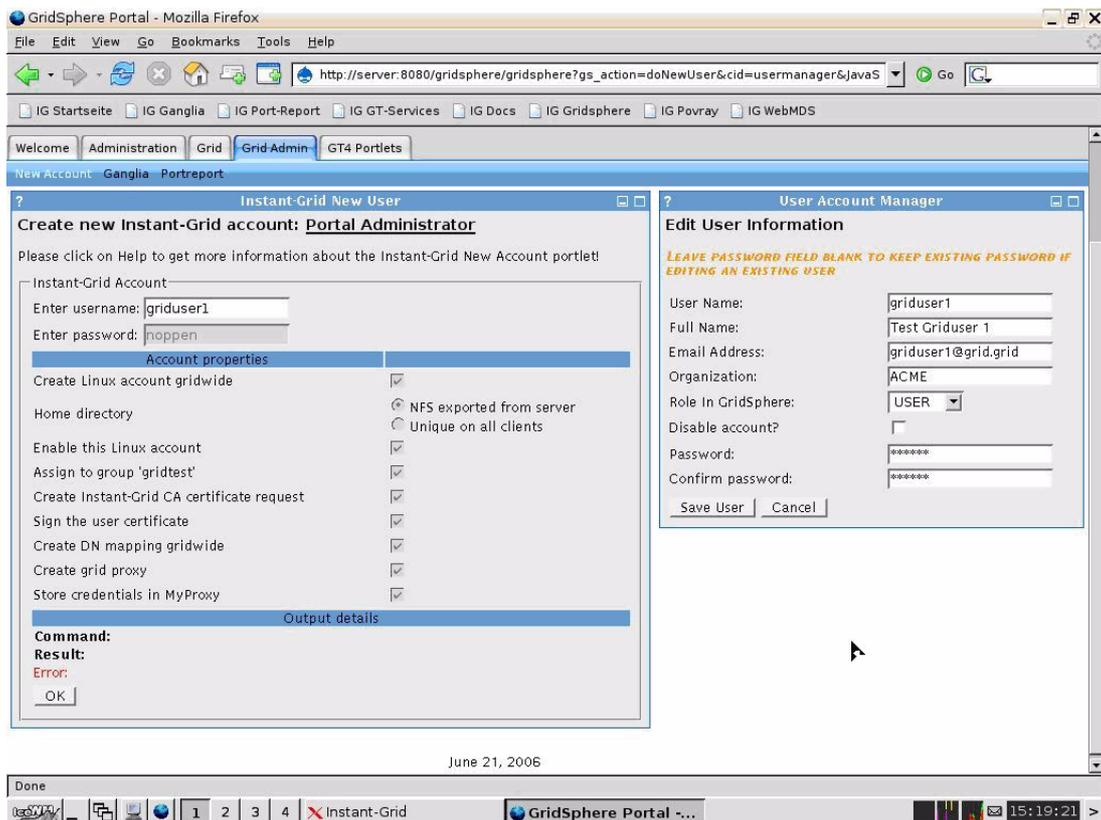


Abb. 3: Das Benutzerverwaltungs-Portlet von Instant-Grid

Eine Portlet-Anwendung zur Grid-Benutzerverwaltung ist in Instant-Grid implementiert (s. Abb. 3). Normalerweise basiert Gridsphere auf einer eigenen Benutzerverwaltung und besitzt keine Schnittstelle zur Benutzerdatenbank des Betriebssystems. Daher müssen Grid-Nutzer für gewöhnlich sowohl auf Gridsphere-Ebene als auch auf der Ebene des Betriebssystems verwaltet werden. Der Grid-Administrator hat in dem Fall die notwendige Zuordnung für die Nutzer auf beiden Ebenen vorzunehmen. Dann muss der CA-Administrator Zertifikate für neu hinzukommende Benutzer ausstellen. Danach wird der Benutzer im Normalfall sein eigenes Grid-Credential erzeugen und dieses Online in ein entsprechendes Repository für derartige Credentials einfügen (MyProxy). Das Benutzerverwaltungs-Portlet von Instant-Grid ermöglicht es, all diese Schritte gemeinsam und transparent durchzuführen: die Portal-Besucher können neue Betriebssystem- und Portal-Benutzerkonten in wenigen Schritten anlegen - ohne jedes Hintergrundwissen über Benutzerverwaltung oder die Sicherheits-Infrastruktur im Grid.

Darüber hinaus gibt es weitere Portlet-basierte Web-Anwendungen: Grid-Portlets können für das Submittieren von Jobs verwendet werden. Es gibt die Möglichkeit für Datei-Transfer und das Verwalten von Credentials im Instant-Grid, womit die wesentlichsten Portlets zum Betrieb eines Grid-Port-

tals in einer Produktionsumgebung bereitgestellt sind.

Die Informationen über die im Instant-Grid verfügbaren Dienste können von MDS4 über eine Webseite (Web-MDS) [9] oder ein Grid-Portlet innerhalb des auf Gridsphere basierenden Portals abgerufen werden. Alle Globus-Dienste, und damit auch alle Klienten, melden sich wiederholt etwa alle fünf Minuten automatisch beim Index-Dienst auf dem Frontend. Alternativ werden sie auf Anfrage durch den Index-Dienst des Frontend aufgefordert, sich zurückzumelden. In beiden Fällen müssen die Dienste so konfiguriert sein, dass sie den Frontend kennen, was ebenfalls, wie zuvor beschrieben, während des Boot-Vorgangs automatisch eingerichtet wird. Der Status der verfügbaren Dienste von Instant-Grid ist damit nach spätestens fünf Minuten aktualisiert.

3.2.5 Sicherheit

Bei Live-CDs ist es übliche Praxis, einen festen und bekannten Benutzer für die Anmeldung zu verwenden, und ebenso wird normalerweise jeder externe Login mit diesem Benutzernamen aus Sicherheitsgründen unterbunden. Dieser Praxis wurde auch bei Instant-Grid entsprochen. Die Web-Services (Globus Gatekeeper, Web-Service-Container etc.) sind so konfiguriert, dass sie unter einem eigenen gesperrten System-Account arbeiten (globus). Das Instant-Grid-Netzwerk ist durch eine Firewall

geschützt, die den direkten Zugang von der Außenwelt unmöglich macht. Die Klienten sind aber durchaus mittels NAT über den Frontend-Knoten (siehe 3.2.2) in der Lage, mit der Außenwelt zu kommunizieren. Instant-Grid kann damit als isolierte Test-Umgebung betrieben werden.

Die Grid-Sicherheits-Infrastruktur (GSI) des Globus-Toolkits, die auch Instant-Grid verwendet, wurde durch das Global Grid Forum (GGF) [10] und die Internet Engineering Task Force (IETF) [11] als Standard-Sicherheits-Infrastruktur anerkannt. Ein Ziel von Instant-Grid ist es, dass, sobald neue Einheiten, wie Nutzer, Dienste oder Ressourcen im Grid erscheinen, diese ein entsprechendes X.509-Zertifikat durch die Instant-Grid Zertifizierungsstelle, basierend auf der SimpleCA [12], ausgestellt und signiert bekommen. Dies geschieht völlig automatisiert und gänzlich ohne Interaktion des Benutzers oder Administrators. Die Zertifikats-Verwaltung beruht dabei auf der CA-Funktionalität von

OpenSSL. Sobald ein neuer Rechner im Instant-Grid gestartet wird oder ein neuer Nutzer angelegt wird, wird nicht nur die Benutzer-Datenbank oder das Hostfile aktualisiert, sondern Rechner oder Nutzer bekommen im gleichen Zuge ein X.509-Zertifikat durch die Instant-Grid-CA ausgestellt. Für den Nutzer werden außerdem Grid-Proxy-Credentials erzeugt, und im MyProxy-Repository abgelegt.

3.2.6 Monitoring und Testing

Im Gegensatz zu Cluster-Umgebungen, bei denen von einem statischen Aufbau ausgegangen wird, verändern sich die verfügbaren Ressourcen im Grid dynamisch während der Nutzung. Daher werden Monitoring-Dienste benötigt, um Kenntnis vom Status der Dienste und der Ressourcen im Grid zu erhalten. Zudem sind spezielle Test-Verfahren vorhanden, um festzustellen, ob die zuvor entdeckten Ressourcen und Dienste einwandfrei arbeiten.



Abb. 4: Monitoring von Instant-Grid mit Ganglia

Instant-Grid nutzt Ganglia [13] zum Monitoring der Hardware (s. Abb. 4) und das Web-Service-basierte Monitoring and Discovery System [9] (MDS4) des Globus Toolkit, um Informationen über vorhandene Dienste zu sammeln. Sowohl Ganglia als auch MDS4 werden während des Boot-Vorgangs gestartet und arbeiten im Hintergrund. MDS4 verwendet die Standard-Konfiguration und die Informationen sind über einen Jakarta Tomcat Server zugänglich. Dieses Setup ist vollständig im Boot-Vorgang von Instant-Grid integriert, womit nach dem Start ein funktionsfähiges MDS4 zur Verfügung steht.

Ein weiterer Monitoring-Test prüft diejenigen offenen Ports, die nach dem Start der Dienste von Instant-Grid erwartet werden. Dies ist ein schneller Test zum Antwortverhalten auf den fraglichen Ports, der keine Aussage über die Dienste machen lässt, die sich hinter diesen Ports verbergen. Die Ergebnisse dieses Tests werden als lokale Webseite präsentiert.

Um die Ressourcen und Dienste zu testen, die durch das Monitoring erkannt wurden, besitzt Instant-Grid eine Reihe von Test-Applikationen. Die Ausgabe dieser Tests wird auf Plausibilität und Richtigkeit überprüft. Zudem wird diese Ausgabe genutzt, um die Information dem Nutzer in einheitlicher und übersichtlicher Weise darzustellen.

3.2.7 Deployment

Während des Boot-Vorgangs kann für jeden Globus-Dienst angegeben werden, ob er gestartet werden soll oder nicht, oder ob ein Paket von Diensten aktiviert werden soll. Dadurch lässt sich Instant-Grid als eine Möglichkeit zum Verteilen von Grid-Middleware nutzen, und gibt dem Nutzer die Gelegenheit, Instant-Grid während des Boot-Vorgangs an die eigenen Wünsche anzupassen. Alle gestarteten Globus-Dienste werden automatisch bei einem Index-Dienst auf dem Frontend registriert. Dabei werden Methoden entsprechend dem Web Service Resource Framework (WSRF) [14] verwendet. Die Informationen über die dann im Instant-Grid verfügbaren Dienste können wie in Abschnitt 3.2.4 beschrieben über ein Grid-Portlet innerhalb des auf Gridsphere basierenden Portals abgerufen werden.

Der übliche Weg zur Verteilung der Instant-Grid-CD ist die in [15] angebotene Download-Seite bzw. die direkte Verteilung vorgepresster CDs. Für die interne Bearbeitung der einzelnen Softwarekomponenten durch verschiedene Partner des Projektes ist es notwendig gewesen, ein Versionierungsverfahren für Instant-Grid einzuführen. Eine Versionierung lässt sich dabei auf verschiedenen Stufen der Softwareintegration durchführen. Das Vorhalten verschiedener vollständig integrierter Versionen von

Instant-Grid-CDs ist zwar die technisch einfachste Möglichkeit, beinhaltet allerdings nur eine sehr grobgranulare Versionskontrolle der Software-Bestandteile. Bei Mitarbeit einer Vielzahl von Personen über Institutionsgrenzen hinweg ist es unerlässlich, die Veränderungen einzelner Codesegmente wesentlich feingranularer recherchierbar zu machen, um eine bessere Kontrolle über die Ursachen bei komplexem Fehlverhalten von Software zu bekommen. Daher war eine Versionskontrolle auf Dateibasis notwendig. Als Versionskontrollsystem wird dabei Subversion [16] verwendet. Über einen HTTP-Port haben die Partner des Projektes direkten Zugang zu den darin versionierten Dateien.

Das Problem bei diesem Vorgehen bei Instant-Grid besteht nun in der Heterogenität der Softwarekomponenten und der Vielzahl der Einzeldateien, die sich auf eine Gesamtgröße von derzeit ca. 2 GB für das gesamte Instant-Grid-System beläuft. Eine Versionierung über eine derartige Daten- und Dateimenge wird schon beim ersten Einspeisen der Daten in das Versionskontrollsystem unübersichtlich und stößt an dessen Leistungsgrenzen. Von den Dateien in Instant-Grid besteht der überwiegende Teil aus dem Basissystem der Knoppix-Live-CD sowie den Komponenten großer Softwarepakete wie z. B. Globus, Ganglia oder Gridsphere, von denen nur ein Bruchteil überhaupt innerhalb des Projektes geändert wird. Wesentlich für die Anpassung dieser Software an Instant-Grid sind im Allgemeinen nur die Dateien, an denen direkt für die Systemintegration und -konfiguration gearbeitet wird. Eine Herausforderung für die Versionskontrolle in diesem Kontext war es daher, einerseits die Konfigurationsdateien für die Softwarekomponenten zusammen mit den spezifischen Systemdateien für Instant-Grid versionierbar zu machen und von der Knoppix-Basis und den Softwarekomponenten zu trennen, andererseits sie aber durch einen automatisierten Workflow wieder zu einer funktionsfähigen CD vereinigen zu können, bei der alle vorher eingestellten Konfigurationen korrekt übernommen werden. Als ein nützliches Hilfsmittel dafür hat sich der Debian-Paketmanager erwiesen.

Im Laufe dieses Versionierungsprozesses stellte sich daher zunehmend die Notwendigkeit zur Modularisierung und Paketierung von Teilen von Instant-Grid heraus. Dieser Prozess ist für einzelne Bereiche, wie zum Beispiel Globus Toolkit, bereits erfolgreich durchgeführt. Er soll allerdings noch auf andere Komponenten ausgeweitet werden.

Obwohl die Modularisierung durch Fragen der Versionskontrolle und des Deployment der Software angestoßen wurde, können sich nun in Zukunft mit einem solchen Konzept neue Möglichkeiten bieten,

die weit über Vereinfachung der internen Administration und Fehlerkontrolle hinausgehen. Daher soll in Folge verstärkt an einer weiteren Modularisierung von Instant-Grid gearbeitet werden. Insgesamt kann dadurch eine neue Flexibilität erreicht werden, die es möglich macht, für spezielle Einsatzzwecke angepasste Speziallösungen anzubieten, die den besonderen Anforderungen der verschiedenen an Grid-Technologie interessierten Communities gerecht wird, und ihnen so einen leichten ersten Einstieg in das Grid ermöglicht.

3.3 Verteiltes Rendern im Grid mit POV-Ray

Eine Applikation innerhalb des Instant-Grid ist das frei verfügbare Raytracingprogramm „The Persistence of Vision Raytracer“ (POV-Ray) [17]. Raytracing ist eine per se leicht parallelisierbare Rendertechnik. Daher wird POV-Ray in Clusterumgebungen oft für Benchmarks und zu Demonstrationszwecken eingesetzt. In Instant-Grid wurde POV-Ray ausgewählt, um dem Benutzer einerseits einen Eindruck über die dynamische Ressourcenverwaltung bei Grids zu veranschaulichen und andererseits, um ihm die Möglichkeit zu geben, auf einfache Weise eine „Renderfarm“ für die Berechnung langwieriger und komplexer Szenen aufzubauen. In diesem Abschnitt wird die Funktionsweise von POV-Ray in Instant-Grid beschrieben.

Eine parallele Funktionsweise von POV-Ray kann dadurch erreicht werden, dass unterschiedliche Knoten des Instant-Grids nur einen Bildausschnitt für eine Berechnung zugewiesen bekommen. Diese werden zur selben Zeit berechnet und anschließend nach erfolgreicher Berechnung zusammengesetzt, um das gesamte Bild zu erhalten.

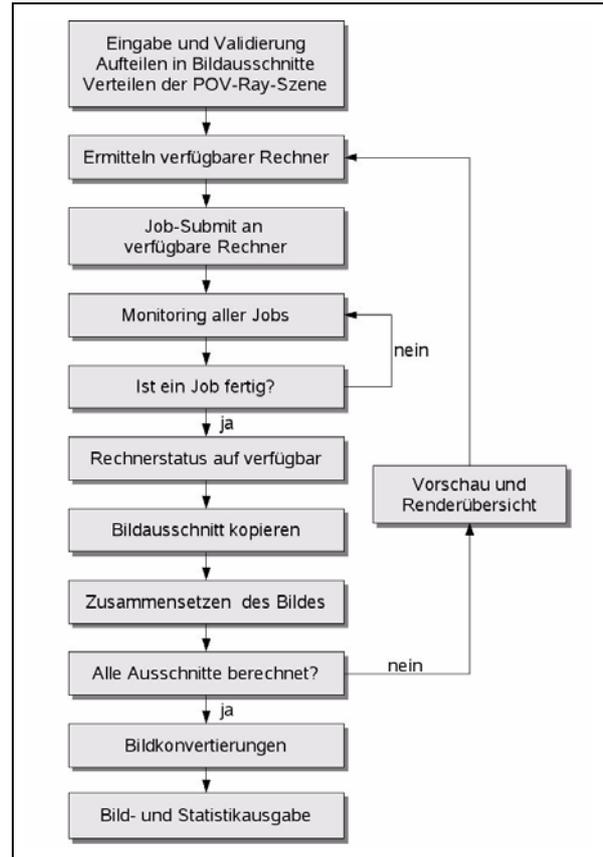


Abb. 5: Schema der Renderprozedur

Die Kommunikation zwischen dem Benutzer und POV-Ray ist mit Hilfe eines auf PHP und Apache basierenden Webfrontends realisiert, auf dem der Benutzer alle nötigen Parameter eingeben kann. Diese beinhalten zum Beispiel den Dateinamen der zu berechnenden Szenendatei und Einstellungen zur Renderqualität. Abb. 5 zeigt eine schematische Darstellung der Renderprozedur. Nachdem die angegebenen Parameter validiert wurden, werden alle für eine Berechnung zur Verfügung stehenden Rechner ermittelt. Hierbei wird auf das Ressourcenmanagement des Instant-Grid zurückgegriffen (siehe Abschnitt 3.2.2). Im Detail wird eine Datei namens „/usr/bin/machines“ überprüft, die alle 30 Sekunden aktualisiert wird und die Namen der Rechner des Instant-Grids beinhaltet. Diese Überprüfung erfolgt während des gesamten Renderprozesses, wodurch sichergestellt wird, dass neu hinzukommende oder nicht mehr verfügbare Rechner erkannt werden und in den Renderprozess integriert oder aus ihm entfernt werden. Per GridFTP (siehe Abschnitt 2.3) wird die zu berechnende Szene an alle Rechner verteilt und anschließend erhält jeder Rechner die Anweisung, einen 50 Pixel hohen Bildabschnitt zu berechnen. Dies wird erreicht, indem ein Job an den Execution Service des jeweiligen

Rechners submittiert wird. Der Execution Service auf den Rechnern ist der in GT4 enthaltene WS-GRAM-Dienst [18]. Dieser wird während des Bootens auf allen Rechnern des Instant-Grids automatisch konfiguriert und gestartet. Während des gesamten Renderprozesses werden alle submittierten Jobs beobachtet und nach erfolgreicher Beendigung eines Jobs wird der berechnete Bildausschnitt per GridFTP auf den Frontend übertragen. Der Klient erhält daraufhin einen neuen Bildausschnitt zur Berechnung zugewiesen. Wenn ein Job nicht erfolgreich beendet wird, weil zum Beispiel der entsprechende Rechner nicht mehr verfügbar ist, wird die Berechnung des Bildausschnitts an einen anderen Rechner übertragen, der diese Berechnung übernimmt. Die fertigen Bildausschnitte liegen im unkomprimierten TGA-Format vor, wodurch sich das Gesamtbild durch einfaches Addieren der Bildausschnitte erzielen lässt.

Der gesamte Renderprozess wird überwacht, indem eine Datei beobachtet wird, die die Start- und Endzeilen aller Bildausschnitte und die Information enthält, ob dieser noch nicht berechnet, fertig berechnet oder einem Klienten zugewiesen wurde. Diese Datei wird beim Starten des Renderprozesses generiert und bei jeder erfolgreichen Beendigung eines Jobs und bei jeder (Neu-)Zuweisung eines Bildausschnittes an einen Klienten aktualisiert. Fertig berechnete Bildausschnitte werden im laufenden Renderprozess zusammengesetzt und dem Benutzer als Vorschau-Bild zusammen mit Statusinformationen zu den einzelnen Rechnern angezeigt. Nachdem alle Bildausschnitte berechnet wurden, wird das Bild zusammengesetzt und auf einer neuen Webseite dargestellt. Eine Statistik gibt Auskunft darüber, welcher Rechner welche Bereiche berechnet hat und wie lange der Renderprozess gedauert hat. Auf dieser Webseite hat der Benutzer außerdem die Möglichkeit, das fertige Bild in unterschiedlichen Bildformaten abzuspeichern.

3.4 Zusammenfassung und Ausblick

Die Instant-Grid-CD kombiniert das etablierte Konzept einer Live-CD mit dem PXE-Startmechanismus und einer automatisierten Verteilung der Globus-Toolkit Grid-Middleware. Man erhält so eine vorkonfigurierte Grid-Umgebung mit der sich Grid-Anwendungen entwickeln, testen und demonstrieren lassen. Darüber hinaus ist Instant-Grid mittels des Gridsphere-Webportals und fertiger Beispielanwendungen auch für hinsichtlich Grid-Computing unerfahrene Nutzer einsetzbar, die sich mit seiner Hilfe mit den Möglichkeiten dieser Technologie vertraut machen können.

Die erste Beispielanwendung ist eine Renderfarm auf Basis des POV-Ray-Raytracers. Hier werden

mittels PHP dynamische Web-Seiten generiert, die die Globus-Kommandozeilen-Schnittstelle zur Verteilung der Render-Aufgaben, zum Datentransfer und zur Kontrolle des Arbeitsfortschritts verwenden. Die Ressourcen-Verwaltung von Instant-Grid dient zum Auffinden von bereitstehenden Ressourcen, die sich während einer Render-Aufgabe dynamisch ändern können. Die transparente Verwendung neuer Ressourcen in einem laufenden Render-Job, kurz nachdem sie bereitstehen, und der mit neuen Ressourcen verbundene Geschwindigkeitsgewinn demonstrieren Schlüssel-Vorteile der Grid-typischen Ressourcen-Virtualisierung.

Für Entwickler ist die Implementierung der gesamten Renderfarm, d. h. sowohl der Nutzerschnittstelle als auch des eigentlichen Workflows, mittels PHP beispielhaft für die Möglichkeit, auf diese Weise einfache Workflows Grid-bereit und nutzerfreundlich zu gestalten, ohne sich zunächst mit Webportal- und Webservice-Entwicklung beschäftigen zu müssen. Letzterer Ansatz ist allerdings deutlich flexibler, weshalb zukünftige Versionen von Instant-Grid auch eine mittels dieser Techniken realisierte Renderfarm enthalten werden. Zudem werden neue Anwendungen zur Demonstration weiterer Grid-Eigenschaften und -Vorteile hinzukommen. Dazu gehören z. B. Zusammenarbeit und die transparente Verteilung komplexer Workflows.

Danksagung

Die Autoren danken dem Bundesministerium für Bildung und Forschung für die Förderung des Instant-Grid-Projektes (Förderkennzeichen 01AK807), den am Projekt beteiligten Partnern Fraunhofer-Institut für Rechnerarchitektur und Softwaretechnik und ed-media und den GWDG-Mitarbeitern T. Ehlers, J. Engelhardt, O. Haan, T. Kálmán, D. Sommerfeld und A. Willner.

Literatur

- [1] The Anatomy of the Grid: Enabling Scalable Virtual Organizations. I. Foster, C. Kesselman, S. Tuecke. International J. Supercomputer Applications, 15(3), 2001.
- [2] German Federal Ministry of Education and Research. eScience Initiative. <http://www.bmbf.de/en/298.php>, 2005.
- [3] W. Gentsch. D-Grid, an e-Science-Framework for Germany. <http://www.d-grid.de/index.php?id=57&L=1>, 2005.
- [4] K. Knopper. Website of Knoppix. <http://www.knoppix.org/>, 2006.
- [5] Foster, I. (2005). Globus Toolkit version 4: Software for service-oriented systems. Network

- and Parallel Computing, Proceedings, Lecture Notes in Computer Science, 3779, 2 - 13
- [6] The Globus Alliance. Globus Toolkit 4 GridFTP Information Webpage. <http://www.globus.org/toolkit/docs/4.0/data/gridftp/>, 2006.
- [7] The Globus Alliance. Globus Toolkit 4 Reliable File Transfer Service Information Webpage. <http://www.globus.org/toolkit/docs/4.0/data/rft/>, 2006.
- [8] Gridsphere. Gridsphere Portal Framework. <http://www.gridsphere.org/>, 2006.
- [9] The Globus Alliance. Globus Toolkit 4 WebMDS Information Webpage. <http://www.globus.org/toolkit/docs/4.0/info/webmlds/>, 2006.
- [10] Global Grid Forum (GGF). Grid Security Infrastructure (GSI) Working Group Grid Forum Security Area. <https://forge.gridforum.org/projects/gsi-wg/>, 2004.
- [11] The Internet Engineering Task Force (IETF). RFC 3820. <http://www.ietf.org/rfc/rfc3820.txt>, June 2004
- [12] The Globus Alliance. Credential Management: SimpleCA. <http://globus.org/toolkit/docs/4.0/security/simpleca/>, 2006.
- [13] The Ganglia Team. Ganglia monitoring system. <http://ganglia.sourceforge.net/>, 2006.
- [14] K. Czajkowski, D. F. Ferguson, I. Foster, J. Frey, S. Graham, I. Sedukhin, D. Snelling, S. Tuecke, W. Vambenepe. The WS-Resource Framework. March 5, 2004.
- [15] Instant-Grid Project. Website of the Instant-Grid Project. <http://www.instant-grid.de/>, 2006.
- [16] Subversion. A version control system, <http://subversion.tigris.org/>, 2006
- [17] POV-Ray - The Persistence of Vision Raytracer. Website of the POV-Ray Project. <http://www.povray.org/>, 2006.
- [18] The Globus Alliance. Globus Toolkit 4 WS-GRAM Information Webpage. <http://www.globus.org/toolkit/docs/4.0/execution/wsgram/>, 2006.

Boehme, Félix, Neumair, Schwardmann

4. Der neue Gastzugang im GÖNET

Zunehmend wird an die GWDG der Wunsch herangetragen, Gästen in den Instituten einen einfachen Zugang zum Internet zu ermöglichen. Oft lassen sich diese Wünsche nur mit einigem Aufwand im GÖNET realisieren. Mit einer neuen Struktur können wir nun diesen Aufwand minimieren; denn auch der einfache Zugang für Gäste bei Veranstaltungen und Tagungen innerhalb der Universität muss durch eine entsprechende Infrastruktur im GÖNET abgedeckt sein.

Bislang haben wir in wenigen zentralen Bereichen der Universität bestimmte Netzbereiche für die Gastzugänge eingerichtet. Diese sind meist Teil des institutseigenen Netzes. Bei deren Nutzung ist aber auch der Zugriff auf interne Ressourcen möglich, was nicht immer wünschenswert ist. Überdies ist die bisherige Struktur nicht ausreichend durch Firewalls abgesichert.

Wir haben seit Anfang September einen vollkommen neuen Gastzugang für das gesamte GÖNET eingerichtet, welcher einige wesentliche Verbesserungen mit sich bringt.

4.1 Die Problematik

Gerade die Einrichtung von Netzzugängen für Gäste stellt nicht zuletzt aus sicherheitstechnischer Sicht eine größere Herausforderung an den Netzbetreiber dar. Hier muss der Spagat zwischen möglichst barrierefreiem Zugang und hoher Sicherheit des internen Netzwerkes geschaffen werden. Überdies sollte der Schutz des Gastes und damit auch seiner Daten bei Nutzung des Netzwerkes im Vordergrund stehen. Die GWDG darf unbekanntem Personenkreisen nicht beliebig den Zugang zum Internet ermöglichen, da die Internetnutzung zum DFN zweckgebunden ist. Gerade auch diesem Umstand muss die neue Lösung Rechnung tragen.

Eine weitere Problematik sahen wir in einigen Instituten, welche auf verschiedene Weise Gastzugänge im eigenen Netz realisiert hatten, oft unter ungünstigen Bedingungen und meist zu Lasten der eigenen Netzwerksicherheit.

Dem Wunsch einiger Institute der Universität Göttingen, einen sicheren Zugang für deren Gäste zu bekommen, können wir nun mit der neuen Lösung besser als vorher begegnen.

4.1.1 Was sind Gäste?

Gäste sind Personen, welche die Infrastruktur des Internet nutzen können, gleichzeitig aber keinen oder nur eingeschränkten Zugriff auf das interne Institutsnetz und deren Ressourcen besitzen. Darüber hinaus sind Gäste auch Personen, die nur für einen zeitlich begrenzten Zeitraum das Netzwerk nutzen.

4.2 Der neue Gastzugang

Nicht zuletzt auch motiviert durch die kürzlich in Betrieb gegangenen Firewallmodule (s. die GWDG-Nachrichten 2/2006) sowie dem IPS (Intrusion Prevention System) bei der GWDG (s. die GWDG-Nachrichten 7/2006 und 8/2006) konnten wir einen umfangreicheren Zugang für die Gäste der Universität einrichten.

4.2.1 Wer kann den Zugang nutzen?

Prinzipiell können alle Institute der Universität den Zugang in Anspruch nehmen. Dieser kann entweder dauerhaft eingerichtet sein oder zeitlich begrenzt im Rahmen von Veranstaltungen und Tagungen installiert werden.

4.2.2 Der Aufbau

Anforderungen

Die Anforderungen an den Gastzugang, der innerhalb des gesamten GÖNET erreicht werden kann, sind:

1. Strikte Trennung zwischen internem Netzwerk und dem Gastnetzwerk.
2. Zugriff der Gäste auf Ressourcen des GÖNET soll nur in Ausnahmefällen möglich sein.
3. Der Zugriff auf das Internet aus dem Gästernetz muss derart gesichert werden, dass unerlaubte Nutzung nicht möglich ist oder mindestens erschwert wird. Missbräuchliche Nutzung kann u. a. der Betrieb von Tauschbörsen mit illegalem Inhalt oder das Attackieren anderer Systeme sein.
4. Schutz des Gästernetzes: Ein Zugriff von außen auf interne Rechner im Gästernetz ist prinzipbedingt nicht möglich. Dadurch können auch keine Server oder Dienste, die aus dem Internet erreicht werden sollen, im Gästernetz betrieben werden.
5. Automatische IP-Addressvergabe durch DHCP: Ein DHCP-Server im Gästernetz sorgt für die dynamische Vergabe von IP-Adressen.

6. Überwachung der Aktivitäten im Gästernetz hinsichtlich Bandbreite und Fehlnutzung: Eine genauere Betrachtung bezüglich Fehlnutzung des Gästernetzes soll automatisch erfolgen und im Ausnahmefall der Zugang für den/die verursachenden Rechner gesperrt werden.
7. Möglichst einfacher Anschluss des Gast-PCs an das Netz.
8. Zentrales Management für das Gästernetzwerk.

Das Gästernetz wird im Wesentlichen aus den folgenden Komponenten gebildet. Mit diesen Komponenten lassen sich alle o. g. Punkte im neuen Gästernetz realisieren.

- zentraler Firewall auf dem Router der GWDG
- IPS bei der GWDG
- DHCP-Server auf der Firewall sowie als externer Server
- VLAN-Struktur
- zentrales Management

VLAN-Struktur

Den wesentlichen Baustein der Gästernetzes bildet ein neues VLAN (Virtual LAN) im GÖNET, welches explizit zur Nutzung als Gastzugang an wesentlichen Knotenpunkten bereits eingerichtet ist. Durch das VLAN wird das Gastnetz auf Layer2 vollständig vom übrigen GÖNET/Institutsnetz getrennt. Dadurch ist die entscheidende Anforderung in Punkt 1 gelöst. Jeder im GÖNET eingesetzte Switch ist in der Lage, VLANs zu „verstehen“. Dadurch können wir Teile (bestimmte Ports) eines Switches zu einer Gruppe zusammenführen und durch das Gast-VLAN getrennt vom internen Institutsnetz weiterleiten. Eine Kommunikation zwischen den VLANs ist nicht möglich.

Firewall und interne IP-Adressen

Für den Schutz des Gästernetzes sorgt eine zentrale Firewall. Als Basisregeln sind alle Zugriffe von innen zum Internet erlaubt, alle Zugriffe vom Internet nach innen jedoch verboten.

NAT (Network Address Translation)

Zusätzlich werden im internen Gästernetz IP-Adressen aus dem „Private Network“ vergeben, welche durch NAT hinter der Firewall im Internet als speziell für den Gastzugang vorgesehene IP-Adressen übersetzt werden. Dadurch erreichen wir eine grö-

ßere Flexibilität und sind nicht auf die Anzahl der verfügbaren IP-Adressen im GÖNET beschränkt.

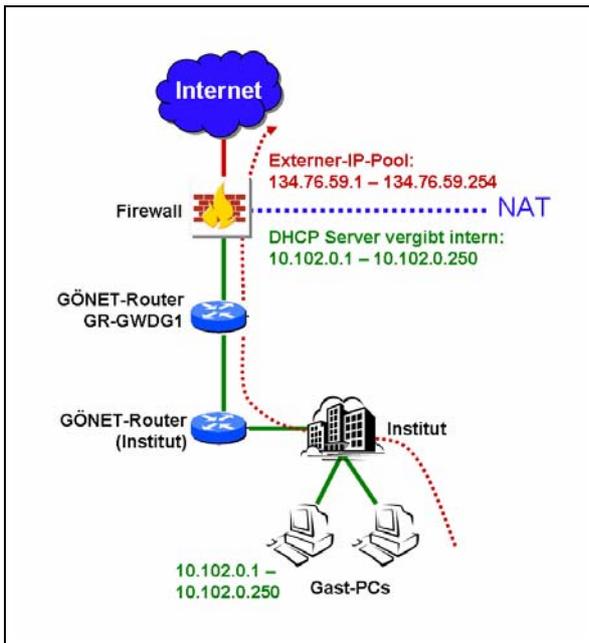


Abb. 1

Abb. 1 verdeutlicht den Zusammenhang zwischen dem NAT-Mapping und der Gesamtstruktur des Gästernetzes.

Für den Gastzugang steht ein externer IP-Address-Pool von 254 Adressen zur Verfügung. Es sind dies die Adressen 134.76.59.1 – 134.76.59.254. Ein Gastbenutzer ist demnach im Internet mit einer Adresse aus diesem Pool sichtbar. Innerhalb des Gästernetzes besitzt der Benutzer eine IP-Adresse aus dem Bereich 10.102.0.1 – 10.102.0.250, welche via DHCP dynamisch vergeben wird. Sollten wir feststellen, dass der Bereich von intern 250 Adressen nicht ausreicht, werden wir diesen entsprechend vergrößern. Extern werden es aber weiterhin 254 verfügbare Adressen bleiben, sodass bei mehr als 254 gleichzeitigen Benutzern mehrere interne IP-Adressen sich eine externe IP-Adresse teilen (PAT = Port Address Translation), was i. d. R. die Funktionstüchtigkeit des Netzzugangs in keiner Weise beeinträchtigt.

Sichere Nutzung des Gästernetzes

Neben der Firewall, sorgt das zentrale IPS der GWDG für einen entscheidenden Schutz im Netzwerkverkehr aus- und in das Gästernetz.

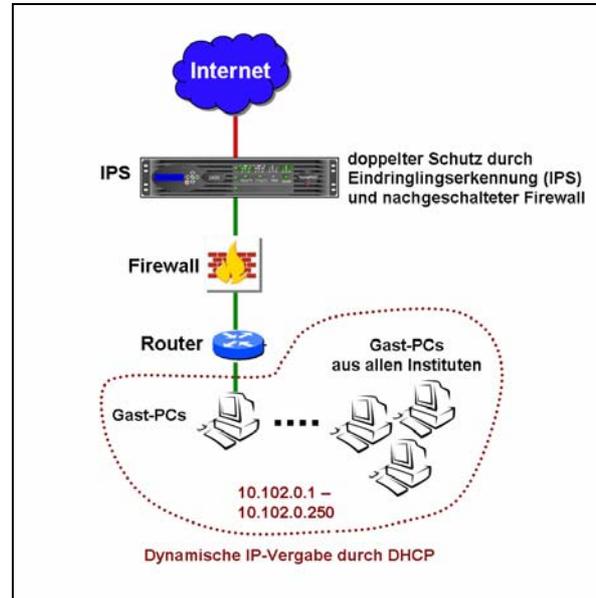


Abb. 2

Abb. 2 zeigt die Struktur und die Integration der Komponenten, die für einen sicheren Zugang sorgen.

Hinter der Firewall ist das IPS angebunden, welches missbräuchliche Nutzung erkennt und automatisch unterbindet. Dadurch ist auch der Betrieb von Tauschbörsen und weiteren illegalen Aktivitäten zumindest sehr erschwert. Das IPS schützt gleichzeitig vor etwaigen Angriffen aus dem Internet und schließt dadurch die Lücke, die eine Firewall alleine nicht einmal erkennt. Dennoch ist die Firewall soweit geöffnet, dass nahezu alle legalen Dienste aus dem Gästernetz heraus nutzbar sind (Mail, Web, FTP, Telnet, SSH u. v. m.). Einzig und allein die Gefährdung innerhalb des Gästernetzes zwischen den Gästen ist noch denkbar, aber nicht zu erwarten.

Schutz des eigenen Rechners erforderlich

Bei der Nutzung des Gästernetzes ist dennoch auf ausreichenden Schutz des eigenen Systems zu achten. Eine „Personal Firewall“ sowie ein aktueller Virens scanner sind nach wie vor zu empfehlen, da andere Gäste sonst bei allzu offenen Systemen Zugriff auf den eigenen Rechner bekommen könnten. Hier unterscheidet sich das Gästernetz nicht von anderen internen Netzstrukturen. Eine Verteilung von Viren ausgehend von einem infizierten Gastrechner ist auch hier möglich, wenngleich die Ausbreitung meist durch das IPS erkannt wird. Dennoch haben wir nicht die Möglichkeit, innerhalb des

Gästenetzes die Kommunikation zwischen zwei Gastsystemen zu unterbinden. Lediglich die Kommunikation ins Internet wird kontrolliert.

4.3 Wie bekomme ich das Gästernetz?

Es existieren drei unterschiedliche Zugangsvarianten:

4.3.1 Permanente Nutzung

Wenn innerhalb des Institutes bestimmte Bereiche für Gäste eingerichtet werden, müssen sich die im Institut zuständigen Netzwerkadministratoren an die GWDG wenden. Dazu benötigen wir die Informa-

tion, welche Ports auf welchen Switches innerhalb des Institutes dafür genutzt werden sollen. Sind anschließend diese Ports von uns auf den Gastsnetzbetrieb umgestellt, können diese nur noch für diesen Zweck verwendet werden. Eine Rückstellung ist natürlich immer noch möglich.

Die folgende Abb. 3 verdeutlicht den Zusammenhang. Hier werden einige Ports eines Switches im Institut durch das Gäste-VLAN vom internen Institutsnetz abgetrennt. Wird am Gast-Port ein Rechner eingesteckt, so läuft die Kommunikation aus dem Institut heraus parallel durch das gesamte GÖNET bis hin zur Firewall bei der GWDG.

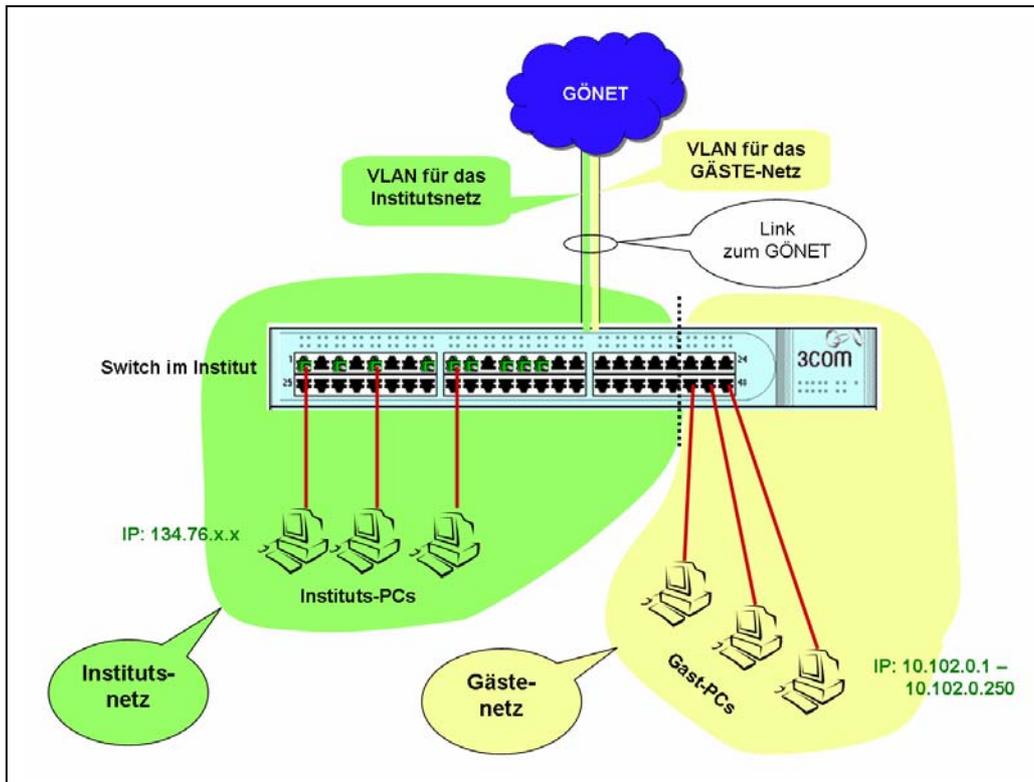


Abb. 3

4.3.2 Vorübergehende Nutzung bei Tagungen, Workshops und weiteren Veranstaltungen

Im Rahmen von Veranstaltungen in den Instituten, zu denen auch Gäste einen Internetzugang benötigen, können wir diese auf den vom Institut genannten Ports für die Dauer der Tagung konfigurieren. Eine Rückstellung der Ports des Switches erfolgt dann nach der Tagung.

4.3.3 Nutzung im ZHG

Im Bereich des Zentralen Hörsaalgebäudes (ZHG) der Universität ist das Gästernetz permanent eingerichtet. Weitere Orte für die sinnvolle Nutzung als

Gastzugang werden wir in Zukunft finden und erweitern.

4.3.4 Was muss der Gast tun?

Für den Gast ist der Zugang ausgesprochen einfach: Sein Rechner muss lediglich auf „*automatisches Beziehen der IP-Adresse*“ eingestellt sein (DHCP). Alles Andere läuft dann automatisch. Eine IP-Adresse aus dem internen Bereich (10.102.0.1 – 250) wird vergeben sowie die DNS-Server der GWDG. Der Benutzer kann sofort ins Internet ohne vorherige Authentifizierung. Damit entsprechen wir dem wichtigen Punkt 7 im Abschnitt 4.2.2.

4.4 Ausblick

Eine Erweiterung des Gastzugangs auch auf das Göttinger Funk-LAN (GoeMobile) ist geplant. Diese sollte mit der geplanten Neustrukturierung des GoeMobile einhergehen. Aufgrund einiger größerer

Veranstaltungen innerhalb der Universität, bei denen die GWDG auch im Funk-LAN einen Gastzugang eingerichtet hatte, werden wir in Zukunft auch diesen Bereich erweitern wollen.

IBleiber

5. Kurse des Rechenzentrums

5.1 Allgemeine Informationen zum Kursangebot der GWDG

5.1.1 Teilnehmerkreis

Das Kursangebot der GWDG richtet sich an die Mitarbeiterinnen und Mitarbeiter aus den Instituten der Universität Göttingen und der Max-Planck-Gesellschaft sowie aus anderen wissenschaftlichen Einrichtungen, die zum erweiterten Benutzerkreis der GWDG gehören. Eine Benutzerkennung für die Rechenanlagen der GWDG ist nicht erforderlich.

5.1.2 Anmeldung

Anmeldungen können schriftlich per Brief oder per Fax unter der Nummer 0551 201-2150 an die

GWDG
Kursanmeldung
Postfach 2841
37018 Göttingen

oder per E-Mail an die Adresse auftrag@gwdg.de mit der Subject-Angabe „Kursanmeldung“ erfolgen. Für die schriftliche Anmeldung steht unter

<http://www.gwdg.de/service/nutzung/antragsformulare/kursanmeldung.pdf>

ein Formular zur Verfügung. Telefonische Anmeldungen können wegen der Einbeziehung der Kurse in die interne Kosten- und Leistungsrechnung der GWDG nicht angenommen werden. Aus diesem Grund können Anmeldungen auch nur durch den Gruppenmanager - eine der GWDG vom zugehörigen Institut bekannt gegebene und dazu autorisierte Person - oder Geschäftsführenden Direktor des Instituts vorgenommen werden. Die Anmeldefrist endet jeweils 7 Tage vor Kursbeginn. Sollten nach dem Anmeldeschluss noch Teilnehmerplätze frei sein, sind auch noch kurzfristige Anmeldungen in Absprache mit dem Dispatcher (Tel.: 0551 201-1523, E-Mail: auftrag@gwdg.de) möglich. Eine Anmeldebestätigung wird nur an auswärtige Institute oder auf besonderen Wunsch zugesendet. Falls eine Anmeldung wegen Überbelegung des Kurses nicht berücksichtigt werden kann, erfolgt eine Benachrichtigung.

5.1.3 Kosten bzw. Gebühren

Die Kurse sind - wie die meisten anderen Leistungen der GWDG - in das interne Kosten- und Leistungsrechnungssystem der GWDG einbezogen. Die bei den Kursen angegebenen Arbeitseinheiten (AE) werden vom jeweiligen Institutskontingent abgezogen. Für die Institute der Universität Göttingen und der Max-Planck-Gesellschaft erfolgt keine Abrechnung in EUR.

5.1.4 Rücktritt und Kursausfall

Absagen durch die Teilnehmer oder die zugehörigen Gruppenmanager bzw. Geschäftsführenden Direktoren können bis zu 8 Tagen vor Kursbeginn erfolgen. Bei späteren Absagen durch die Teilnehmer oder die zugehörigen Gruppenmanager bzw. Geschäftsführenden Direktoren werden die für die Kurse berechneten Arbeitseinheiten vom jeweiligen Institutskontingent abgebucht. Sollte ein Kurs aus irgendwelchen Gründen, zu denen auch die Unterschreitung der Mindestteilnehmerzahl bei Anmeldeschluss sowie die kurzfristige Erkrankung des Kurshalters gehören, abgesagt werden müssen, so werden wir versuchen, dies den betroffenen Personen rechtzeitig mitzuteilen. Daher sollte bei der Anmeldung auf möglichst vollständige Adressangaben inkl. Telefonnummer und E-Mail-Adresse geachtet werden. Die Berechnung der Arbeitseinheiten entfällt in diesen Fällen selbstverständlich. Weitergehende Ansprüche können jedoch nicht anerkannt werden.

5.1.5 Kursorte

Die meisten Kurse finden in Räumen der GWDG oder des Max-Planck-Instituts für biophysikalische Chemie statt. Der Kursraum und der Vortragsraum der GWDG befinden sich im Turm 6, UG des Max-Planck-Instituts für biophysikalische Chemie, Am Fassberg, 37077 Göttingen, der Große Seminarraum im Allgemeinen Institutsgebäude dieses Instituts. Die Wegbeschreibung zur GWDG bzw. zum Max-Planck-Institut für biophysikalische Chemie sowie der Lageplan sind im WWW unter dem URL

<http://www.gwdg.de/gwdg/standort/lageplan>

zu finden. Der gemeinsame Schulungsraum von GWDG und SUB befindet sich im Untergeschoss der Niedersächsischen Staats- und Universitätsbibliothek, Platz der Göttinger Sieben 1, 37073 Göttingen.

5.1.6 Ausführliche und aktuelle Informationen

Ausführliche Informationen zu den Kursen, insbesondere zu den Kursinhalten und Räumen, sowie aktuelle kurzfristige Informationen zum Status der Kurse sind im WWW unter dem URL

<http://www.gwdg.de/service/kurse>

zu finden. Anfragen zu den Kursen können an den Dispatcher per Telefon unter der Nummer 0551 201-1524 oder per E-Mail an die Adresse auftrag@gwdg.de gerichtet werden. Zweimal jährlich wird ein Katalog mit dem aktuellen GWDG-Kursprogramm versendet. Interessenten, die in den Verteiler aufgenommen werden möchten, können dies per E-Mail an die Adresse gwdg@gwdg.de mitteilen.

5.2 Kurse von Oktober bis Dezember 2006 in thematischer Übersicht

EDV-Grundlagen und Sonstiges

| Kurse | Termine | Vortragende |
|--|------------------------------|-----------------------------|
| Broschüreneerstellung, Spezial- und Posterdruck bei der GWDG | • 15.11.2006 | Dr. Heuer, Nolte, Wagenführ |
| Einführung in die Nutzung des Leistungsangebots der GWDG | • 06.12.2006 | Dr. Grieger |
| Einführung in Aufbau und Funktionsweise von PCs | • 31.10.2006 | Eyßell |
| Einführung in die Bedienung von Windows-Oberflächen | • 01.11.2006 - 03.11.2006 | Eyßell |
| Führung durch das Rechnermuseum | • 10.11.2006 • 15.12.2006 | Eyßell Eyßell |

Betriebssysteme

| Kurse | Termine | Vortragende |
|--|---------------------------|-----------------------|
| Schnellkurs UNIX für Windows-Benutzer mit Übungen | • 27.11.2006 - 28.11.2006 | Dr. Bohrer |
| Grundkurs UNIX/Linux mit Übungen | • 17.10.2006 - 19.10.2006 | Hattenbach |
| UNIX für Fortgeschrittene | • 06.11.2006 - 08.11.2006 | Dr. Sippel |
| UNIX/Linux-Arbeitsplatzrechner - Installation und Administration | • 11.12.2006 - 12.12.2006 | Dr. Heuer, Dr. Sippel |
| UNIX/Linux-Server - Grundlagen der Administration | • 13.12.2006 - 14.12.2006 | Dr. Heuer, Dr. Sippel |
| UNIX/Linux - Systemsicherheit für Administratoren | • 15.12.2006 | Dr. Heuer, Dr. Sippel |
| Windows 2000/XP/2003 in kleinen Netzwerken | • 13.11.2006 - 14.11.2006 | Quentin |
| Die Windows-Active-Directory-Domäne | • 15.11.2006 - 17.11.2006 | Quentin |
| Cluster- und Raid-Konfigurationen unter Windows 2003 | • 31.10.2006 | Quentin |

Netze / Internet

| Kurse | Termine | Vortragende |
|-------------------------------------|--------------|-------------|
| Sicherheit im Internet für Anwender | • 01.12.2006 | Reimann |

Grafische Datenverarbeitung

| Kurse | Termine | Vortragende |
|--------------------------------|---------------------------|-------------|
| Photoshop für Fortgeschrittene | • 09.10.2006 - 10.10.2006 | Töpfer |

Sonstige Anwendungssoftware

| Kurse | Termine | Vortragende |
|--|---------------------------|-----------------|
| Einführung in das Computeralgebra-System Mathematica | • 11.10.2006 - 12.10.2006 | Dr. Schwardmann |
| MindMapping mit MindManager | • 05.10.2006 | Reimann |
| Die Kommunikationsplattform Microsoft Exchange Server bei der GWDG | • 20.10.2006 | Reimann |
| PowerPoint | • 09.11.2006 - 10.11.2006 | Reimann |
| Mit StarOffice zum Schwarzen Loch | • 14.11.2006 | Dr. Grieger |

Programmiersprachen

| Kurse | Termine | Vortragende |
|-------------------------------------|---------------------------|---|
| Programmierung von Parallelrechnern | • 28.11.2006 - 30.11.2006 | Prof. Haan, Dr. Boehme, Dr. Schwardmann |

5.3 Kurse von Oktober bis Dezember 2006 in chronologischer Übersicht

| Kurs | Vortragende | Termin | Anmelde- schluss | AE |
|--|-----------------|---|---------------------|----|
| Photoshop für Fortgeschrittene | Töpfer | 09.10.2006 - 10.10.2006 09.30 - 16.00 Uhr | 02.10.2006 | 8 |
| Einführung in das Computeralgebra-System Mathematica | Dr. Schwardmann | 11.10.2006 - 12.10.2006 09.00 - 12.00 Uhr und 13.00 - 16.00 Uhr | 04.10.2006 | 8 |
| Grundkurs UNIX/Linux mit Übungen | Hattenbach | 17.10.2006 - 19.10.2006 09.15 - 12.00 Uhr und 13.30 - 16.00 Uhr | 10.10.2006 | 12 |

| Kurs | Vortragende | Termin | Anmelde- schluss | AE |
|--|---|---|-----------------------------|-----------|
| Die Kommunikationsplattform Microsoft Exchange Server bei der GWDG | Reimann | 20.10.2006 09.15 - 12.00 Uhr und 13.00 - 15.00 Uhr | 13.10.2006 | 4 |
| Cluster- und Raid-Konfigurationen unter Windows 2003 | Quentin | 31.10.2006 09.15 - 12.30 Uhr und 13.30 - 16.15 Uhr | 24.10.2006 | 4 |
| Einführung in Aufbau und Funktionsweise von PCs | Eyßell | 31.10.2006 09.15 - 12.30 Uhr | 24.10.2006 | 2 |
| Einführung in die Bedienung von Windows-Oberflächen | Eyßell | 01.11.2006 - 03.11.2006 09.15 - 12.30 Uhr | 25.10.2006 | 6 |
| UNIX für Fortgeschrittene | Dr. Sippel | 06.11.2006 - 08.11.2006 09.15 - 12.00 Uhr und 13.15 - 15.30 Uhr | 30.10.2006 | 12 |
| PowerPoint | Reimann | 09.11.2006 - 10.11.2006 09.15 - 12.00 Uhr und 13.00 - 15.00 Uhr | 02.11.2006 | 8 |
| Führung durch das Rechner- museum | Eyßell | 10.11.2006 10.00 - 12.30 Uhr | 03.11.2006 | 0 |
| Windows 2000/XP/2003 in kleinen Netzwerken | Quentin | 13.11.2006 - 14.11.2006 09.30 - 15.30 Uhr | 06.11.2006 | 8 |
| Mit StarOffice zum Schwarzen Loch | Dr. Grieger | 14.11.2006 09.00 - 12.00 Uhr | 07.11.2006 | 2 |
| Die Windows-Active-Directory- Domäne | Quentin | 15.11.2006 - 17.11.2006 09.30 - 15.30 Uhr (am 17.11. bis 13.30 Uhr) | 08.11.2006 | 10 |
| Broschüreneerstellung, Spezial- und Posterdruck bei der GWDG | Dr. Heuer, Nolte, Wagenführ | 15.11.2006 16.15 - 17.45 Uhr | 08.11.2006 | 1 |
| Schnellkurs UNIX für Windows- Benutzer mit Übungen | Dr. Bohrer | 27.11.2006 - 28.11.2006 13.00 - 16.00 Uhr | 20.11.2006 | 4 |
| Programmierung von Parallelrech- nern | Prof. Dr. Haan, Dr. Boehme, Dr. Schwarzmann | 28.11.2006 - 30.11.2006 09.15 - 12.15 Uhr und 13.30 - 16.30 Uhr | 21.11.2006 | 12 |
| Sicherheit im Internet für Anwender | Reimann | 01.12.2006 | 24.11.2006 | 2 |
| Einführung in die Nutzung des Leistungsangebots der GWDG | Dr. Grieger | 06.12.2006 17.00 - 20.00 Uhr | 29.11.2006 | 0 |
| UNIX/Linux-Arbeitsplatzrechner - Installation und Administration | Dr. Heuer, Dr. Sippel | 11.12.2006 - 12.12.2006 09.30 - 12.30 Uhr und 13.30 - 16.30 Uhr | 04.12.2006 | 8 |
| UNIX/Linux-Server - Grundlagen der Administration | Dr. Heuer, Dr. Sippel | 13.12.2006 - 14.12.2006 09.30 - 12.30 Uhr und 13.30 - 16.30 Uhr | 06.12.2006 | 8 |

| Kurs | Vortragende | Termin | Anmelde- schluss | AE |
|---|--------------------------|--|---------------------|----|
| UNIX/Linux - Systemsicherheit für Administratoren | Dr. Heuer, Dr. Sippel | 15.12.2006 09.30 - 12.30 Uhr und 13.30 - 15.00 Uhr | 08.12.2006 | 4 |
| Führung durch das Rechner- museum | Eyßell | 15.12.2006 10.00 - 12.30 Uhr | 08.12.2006 | 0 |

6. Betriebsstatistik August 2006

6.1 Nutzung der Rechenanlagen

| Rechner | Zahl der Prozessoren | CPU- Stunden |
|----------------|-------------------------|-----------------|
| DECalpha | 8 | 78,29 |
| IBM Regatta | 124 | 57.764,18 |
| Linux Parallel | 252 | 167.449,46 |
| Linux Opteron | 96 | 63.562,50 |

6.2 Betriebsunterbrechungen

| Rechner/PC-Netz | Störungen | | System- pflege | |
|-----------------|-----------|---------|-------------------|---------|
| | Anzahl | Stunden | Anzahl | Stunden |
| UNIX-Cluster | 0 | | 0 | |
| IBM Regatta | 0 | | 0 | |
| Linux Parallel | 0 | | 0 | |
| Linux Opteron | 0 | | 0 | |
| PC-Netz | 0 | | 0 | |
| Nameserver | 0 | | 0 | |
| Mailer | 0 | | 0 | |

7. Autoren dieser Ausgabe

| Name | Artikel | E-Mail-Adresse / Telefon-Nr. |
|----------------------------|--|---|
| Dr. Christian Boehme | <ul style="list-style-type: none"> Instant-Grid: Demonstration, Entwicklung und Test von Grid-Anwendungen | cboehme1@gwdg.de 0551 201-1839 |
| Andreas Félix | <ul style="list-style-type: none"> Instant-Grid: Demonstration, Entwicklung und Test von Grid-Anwendungen | afelix@gwdg.de 0551 201-1906 |
| Sigrun Greber | <ul style="list-style-type: none"> Kontingenzuweisung für das vierte Quartal 2006 | sgreber@gwdg.de 0551 201-1518 |
| Andreas Ißleiber | <ul style="list-style-type: none"> Der neue Gastzugang im GÖNET | aisslei@gwdg.de 0551 201-1815 |
| Prof. Dr. Bernhard Neumair | <ul style="list-style-type: none"> Instant-Grid: Demonstration, Entwicklung und Test von Grid-Anwendungen | Bernhard.Neumair@gwdg.de 0551 201-1545 |
| Michael Reimann | <ul style="list-style-type: none"> Relay-Sperre des GWDG-Mailers | Michael.Reimann@gwdg.de 0551 201-1826 |
| Dr. Ulrich Schwarzmann | <ul style="list-style-type: none"> Instant-Grid: Demonstration, Entwicklung und Test von Grid-Anwendungen | uschwar1@gwdg.de 0551 201-1542 |

