GWDG NACHRICHTEN

10|12

GWDG-Benutzerraum

Ausbau des Leihrechnerpools

iOS 6

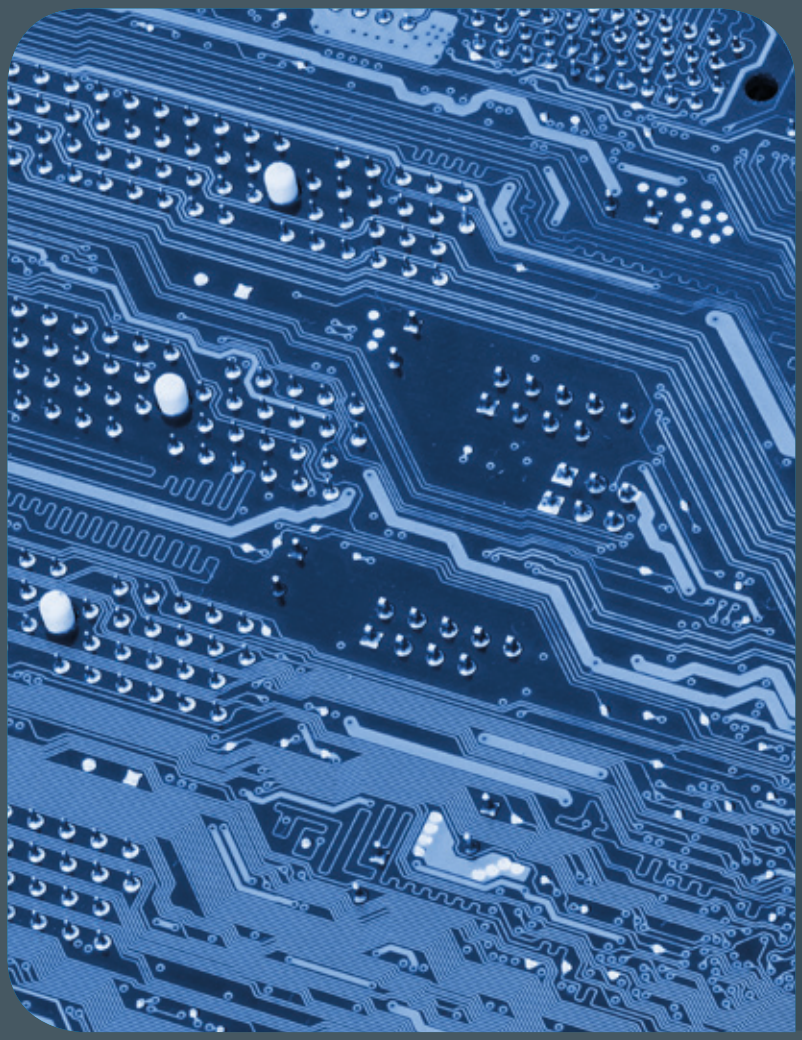
Authentifizierung mit Kerberos

Nacht des Wissens

ZEITSCHRIFT FÜR DIE KUNDEN DER GWDG

GWDG

Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen



GWDG
NACHRICHTEN

10|12

Inhalt

3 **Editorial** 4 **Die Windows-PCs im GWDG-Benutzerraum** 7 **Weiterer Ausbau des Leihrechnerpools der GWDG** 8 **iOS 6 für iPhone und iPad** 11 **Tipps & Tricks** 12 **Kerberos-Authentifizierung von UNIX/Linux-Clients im Active Directory – Teil 3: Die Konfiguration zur „Kerberisierung“ der Clients** 16 **Erste Nacht des Wissens in Göttingen am 24. November 2012** 17 **Personalia** 18 **Kurse**

Impressum

Zeitschrift für die Kunden der GWDG

ISSN 0940-4686
35. Jahrgang
Ausgabe 10/2012

Erscheinungsweise:
monatlich

www.gwdg.de/gwdg-nr

Auflage:
500

Fotos:
© Antrey - Fotolia.com (1)
© Stuart Miles - Fotolia.com (7)
© storm - Fotolia.com (9)
© xiaoliangge - Fotolia.com (11)
MPIbpc-Medienservice (3, 17)
Presse, Kommunikation und Marketing der Universität Göttingen (16)
GWDG (2, 4, 5, 8, 18)

Herausgeber:
Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen
Am Faßberg 11
37077 Göttingen
Tel.: 0551 201-1510
Fax: 0551 201-2150

Redaktion:
Dr. Thomas Otto
E-Mail: thomas.otto@gwdg.de

Herstellung:
Maria Geraci
E-Mail: maria.geraci@gwdg.de

Druck:
GWDG / AG H
E-Mail: printservice@gwdg.de

Prof. Dr. Ramin Yahyapour
ramin.yahyapour@gwdg.de
0551 201-1545

Liebe Kunden und Freunde der GWDG,

am 24. November ist es soweit und die erste „Nacht des Wissens" findet in Göttingen an über 20 Orten statt. Der gesamte Göttinger Wissenschaftsstandort präsentiert sich der breiten Öffentlichkeit. So stellt sich auch die GWDG vor und gibt einen Einblick in aktuelle Themen. Schwerpunkt einer eigenen Präsentation wird dabei die Vorstellung der aktuellen und künftigen Cloud-Angebote der GWDG für die Wissenschaft sein. Neben dem bisherigen GWDG-Cloud-Storage-Dienst „PowerFolder" wird insbesondere die neue GWDG Compute Cloud als Prototyp gezeigt.

Nach umfangreichen Entwicklungsarbeiten für diesen neuen Dienst nähern wir uns zum Ende des Jahres der öffentlichen Beta-Phase für das neue Compute-Cloud-Angebot und können bereits einen Einblick geben, wie der neue Dienst künftig für die Wissenschaft aussehen wird. Beim diesjährigen DV-Treffen der Max-Planck-Institute Mitte dieses Monats fand der Workshop zur GWDG Cloud reges Interesse. Wissenschaftler und IT-Verantwortliche werden durch diesen Dienst in die Lage versetzt, jederzeit schnell und auf einfache Weise eigenständig virtuelle Rechner für die verschiedensten Einsatzzwecke einrichten zu können. Hohe Skalierbarkeit und Effizienz zeichnen den neuen Dienst aus. Wir werden in den kommenden Ausgaben der GWDG-Nachrichten näher über diesen Dienst berichten.

Es würde mich freuen, Sie bei der „Nacht des Wissens" begrüßen zu dürfen. Unsere Mitarbeiterinnern und Mitarbeiter stehen Ihnen gerne für Ihre Fragen zur Verfügung.

Ramin Yahyapour

GWDG – IT in der Wissenschaft

1_PC-Arbeitsplätze im GWDG-Benutzerraum

Die Windows-PCs im GWDG-Benutzerraum

Text und Kontakt:
Uwe Nolte
uwe.nolte@gwdg.de
0551 201-1547

In ihrem Benutzerraum stellt die GWDG ihren Kunden insgesamt 14 Rechner mit verschiedenen Betriebssystemen und einem umfangreichen Softwareangebot zur Verfügung. Diese Rechner können während der Geschäftszeiten von jedem GWDG-Benutzer genutzt werden, ohne dass sie vorher reserviert werden müssen.

Im Benutzerraum der GWDG finden Sie zehn PCs mit Windows 7 Enterprise, zwei iMac-Computer mit Mac OS X sowie zwei Linux-PCs mit OpenSUSE 11.4 (x86_64). Im Folgenden werden die Windows-PCs näher beschrieben. In einer späteren Ausgabe der GWDG-Nachrichten werden die Mac- und Linux-Rechner folgen.

Diese PCs lassen sich in drei Gruppen unterteilen:

- Scanner-PCs: GWDG-B96, GWDG-B097, GWDG-W7-B01 und GWDG-W7-B02
- Grafik- bzw. Statistik-PCs: GWDG-B098, GWDG-B099 und GWDG-B100
- Office-PCs: GWDG-B101, GWDG-B102 und GWDG-B103

Alle diese PCs sind in das Active Directory der GWDG eingebunden. Standardmäßig wird ein Benutzer gegen die Domäne GWDG authentifiziert. Möchte man sich an einer anderen Domäne anmelden (z. B. MPG-BPC), so ist der Domain-Name vor dem Benutzernamen anzugeben und durch einen Backslash von diesem zu trennen (Beispiel: MPG-BPC\hmeier1).

HARDWARE

Bei den PCs GWDG-B096 bis GWDG-B103 handelt es sich um neuere Systeme vom Typ DELL Optiplex 990. Diese sind mit einer Intel Core i5-2500 CPU ausgestattet, welche mit 3,3 GHz getaktet ist. Darüber hinaus besitzen sie 8 GByte RAM, eine 465-GByte-Festplatte sowie einen DVD-Brenner. Auf der von 1,0 bis 7,9 laufenden Windows-Leistungsindex-Skala erreichen die PCs folgende Werte: Prozessor: 7,5, Arbeitsspeicher: 7,6, Grafik: 5,0 und Festplatte: 5,9. Ausgestattet sind die Geräte mit 24“-Bildschirmen, welche eine Auflösung von 1.080 x 1.920 Pixel besitzen.

Bei den Rechnern GWDG-W7-B01 und GWDG-W7-B02 handelt es sich Dell-Precision-490-Workstations mit einer Intel-Xeon- 5120-CPU, welche mit 2,66 GHz getaktet ist. Beide PCs sind mit 4 GByte RAM sowie zwei Festplatten ausgestattet (C: für das Betriebssystem, E: zum temporären Zwischenspeichern von Benutzerdaten wie z. B. gescannte Bilder). Darüber hinaus besitzen sie einen eingebauten CF- und SD-Kartenleser. Beide Geräte erreichen folgende Windows-Leistungsindizes: Prozessor: 6,0, Arbeitsspeicher: 6,0, Grafik: 4,6 und Festplatte: 5,5. Der GWDG-W7-B01 ist mit einem hochwertigen 26“-Bildschirm vom Typ NEC MultiSync LCD 2690WUXi ausgestattet (Auflösung: 1.920 x 1.200 Pixel), der auf Kundenwunsch kalibriert werden kann. Dieser Monitor ist in der Lage, den Adobe-RGB-Farbraum fast vollständig (95 % Farbraumabdeckung) wiederzugeben. Darüber hinaus besitzt der Monitor eine 12 Bit Lookup Table. Da der Monitor von der UGRA zertifiziert wurde, eignet er sich hervorragend für Bildbearbeitung. Der GWDG-W7-B02 besitzt einen 19“-Bildschirm mit 1.280 x 1.024 Pixel Auflösung.

2_Die Scanner-PCs Im GWDG-Benutzerraum

PERIPHERIE

Die Rechner GWDG-B096, GWDG-B097, GWDG-W7-B01 und GWDG-W7-B02 sind mit verschiedenen Scannern ausgestattet. Der GWDG-B096 besitzt einen EPSON GT-2500 Dokumenten-Scanner mit doppelseitigem Einzelblatteinzug, welcher bis zu 50 Seiten im A4-Format automatisch scannen kann. Seine Scanauflösung beträgt 1.200 dpi.

Die Computer GWDG-B097 und GWDG-W7-B01 sind beide mit einem DIN-A3+-Scanner ausgestattet. Beim GWDG-B097 handelt es sich um ein Modell EPSON GT-20000 mit einer Scan-Auflösung von 600 dpi (horizontal) und 1.200 dpi (vertikal). Der GWDG-W7-B01 ist mit einem EPSON EXPRESSION 10000XL-Scanner ausgerüstet. Dieser Scanner ist in der Lage, Vorlagen mit einer Auflösung von 2.400 dpi (horizontal) und 4.800 dpi (vertikal) zu scannen. Als Besonderheit verfügt er über eine Durchlichteinheit. Dadurch ist dieser Scanner auch in der Lage, Dia- und Negativfilme im Kleinbild- und Mittelformat sowie Overheadfolien einzuscannen. Zum Scannen von Dias sind spezielle Masken vorhanden, die es dem Scanner erlauben, mehrere Dias in einem Arbeitsgang zu scannen.

Der Rechner GWDG-W7-B02 ist mit einem Nikon LS4000ED-Filmscanner ausgestattet. Dieser Scanner ist in der Lage, Dias als auch 6er-Negativstreifen im Kleinbildformat mit einer Auflösung von bis zu 4.000 dpi zu scannen. Für den Scanner ist ein Diamagazin verfügbar mit dem 50 Dias automatisch eingescannt werden können.

SOFTWARE

Bei allen o.g. Systemen kommt Windows 7 Enterprise 64 Bit zum Einsatz. Nur der PC GWDG-W7-B02 ist mit dem Betriebssystem Windows 7 Enterprise 32 Bit ausgestattet. Das ist der Grund, warum bei diesem PC nur 3 GByte RAM genutzt werden können, obwohl er mit 4 GByte RAM ausgestattet ist. Auf den Office-PCs sind Microsoft Office 2010 (inkl. Access, Excel, InfoPath, OneNote, Outlook, PowerPoint, Publisher, SharePoint Workspace und Word), Adobe Acrobat Professional 9, OpenOffice 3.2 (inkl. OpenOffice Base, Calc, Draw, Impress, Math und Writer), IrfanView sowie der SSH-Client X-Win32 installiert. Alle Scanner- und Grafik-PCs sind darüber hinaus mit der Adobe Creative Suite Design Standard in den Versionen CS4 bis CS6 ausgestattet. Beim GWDG-B098 ist sogar die Adobe Creative Suite CS5.5 Master Collection installiert. Auf diesem PC finden Sie darüber hinaus noch die Programme ArcGIS 10, AutoCAD, Scribus, Inkscape und Google Earth. ArcGIS finden Sie auch auf dem PC GWDG-W7-B01. Bis auf den Dia-Scanner PC (GWDG-W7-B02) verfügen die o. g. Scanner- und Grafik-PCs auch über die CorelDRAW-Graphics-Suite in der Version X5 bzw. X6.

Auf den Scanner-PCs GWDG-W7-01, GWDG-B096 und GWDG-B097 kommt als Scansoftware die Software EPSON-Scan zum Einsatz. Zur Texterkennung dient auf dem GWDG-B096 die Software ABBY FineReader 11. Beim Dia-Scanner-PC GWDG-W7-B02 setzen wir zum Scannen von Dias und Negativen die Software NikonScan 4 ein. Auf den Rechnern GWDG-B098 und GWDG-B100 finden Sie auch das Programm WinCDEmu, mit dem Sie ISO-Images als virtuelles CD-Laufwerk einbinden können. Auf dem PC GWDG-B099 finden Sie folgende Statistik-Software: JMP 9, R 2.12.1, SAS 9.3, SPSS 20 sowie STATISTICA 10.

Alle Informationen finden Sie auch auf entsprechenden Schildern am jeweiligen PC-Arbeitsplatz sowie auf dem Anmeldebildschirm.

Im Bild 1 befinden sich auf der Tischgruppe von links nach rechts die beiden Grafik-PCs GWDG-B100 und GWDG-B098 sowie der Statistik-PC GWDG-B099. Dahinter – mit der Rückseite zum Betrachter – die Office-PCs GWDG-B101, GWDG-B102 und GWDG-B103. Ganz hinten an der Wand stehen die beiden Linux-PCs gwdg-wb01 und gwdg-wb02.

Im Bild 2 ist die Reihe der Scanner-PCs zu sehen. Von links nach rechts finden Sie den Dia-Scanner-PC GWDG-W7-B02, gefolgt vom Dokumenten-Scanner-PC und danach die beiden PCs mit DIN-A3+-Scannern GWDG-B097 und GWDG-W7-B01.

Die folgenden Tabellen geben Ihnen noch einmal einen Überblick über die auf den zuvor beschriebenen PCs installierte Software:

RECHNER	SCANNER-PC GWDG-B096
Betriebssystem	Windows 7 Enterprise 64 Bit
Grafik	Adobe Creative Suite 5 Design Standard (inkl. Illustrator, InDesign und Photoshop), CorelDRAW Graphics Suite X5, IrfanView
Office	Adobe Acrobat Professional 9, Microsoft Office 2010 (inkl. Access, Excel, InfoPath, OneNote, Outlook, PowerPoint, Publisher, SharePoint, Workspace und Word), OpenOffice 3.2 (inkl. OpenOffice Base, Calc, Draw, Impress, Math und Writer)
Scan-Software	EPSON Scan, ABBY Fine Reader 11 (OCR-Programm)
SSH-Client	X-Win 32
WWW-Browser	Internet Explorer 9, Mozilla Firefox
Peripherie	Scanner EPSON GT-2500 mit Dokumenteneinzug

RECHNER	SCANNER-PC GWDG-B097
Betriebssystem	Windows 7 Enterprise 64 Bit
Grafik	Adobe Creative Suite 5 Design Standard (inkl. Illustrator, InDesign und Photoshop), CorelDRAW Graphics Suite X5, IrfanView
Office	Adobe Acrobat Professional 9, Microsoft Office 2010 (inkl. Access, Excel, InfoPath, OneNote, Outlook, PowerPoint, Publisher, SharePoint, Workspace und Word), OpenOffice 3.2 (inkl. OpenOffice Base, Calc, Draw, Impress, Math und Writer)
Scan-Software	EPSON Scan
SSH-Client	X-Win 32
WWW-Browser	Internet Explorer 9, Mozilla Firefox
Peripherie	A3+-Scanner EPSON GT-20000

RECHNER	SCANNER-PC GWDG-B098
Betriebssystem	Windows 7 Enterprise 64 Bit
GIS	ArcGIS 10
Grafik	Adobe Creative Suite 5.5 Master Collection (inkl. Illustrator, InDesign, Photoshop, Pemiere, Flash u.v.m.), AutoCAD 2011, CorelDRAW Graphics Suite X5, Inkscape, IrfanView, Scribus
Office	Adobe Acrobat Professional 9, Microsoft Office 2010 (inkl. Access, Excel, InfoPath, OneNote, Outlook, PowerPoint, Publisher, SharePoint, Workspace und Word), OpenOffice 3.2 (inkl. OpenOffice Base, Calc, Draw, Impress, Math und Writer)
SSH-Client	X-Win 32
WWW-Browser	Internet Explorer 9, Mozilla Firefox
Sonstiges	WinCDEmu (bindet ISO-Dateien als virtuelles CD-Laufwerk ein)

RECHNER	STATISTIK-PC GWDG-B099
Betriebssystem	Windows 7 Enterprise 64 Bit
Grafik	IrfanView
Office	Adobe Acrobat Professional 9, Microsoft Office 2010 (inkl. Access, Excel, InfoPath, OneNote, Outlook, PowerPoint, Publisher, SharePoint, Workspace und Word), OpenOffice 3.2 (inkl. OpenOffice Base, Calc, Draw, Impress, Math und Writer)
Statistik	JMP 9, R 2.12.1, SAS 9.3, SPSS 20, STATISTICA 10
SSH-Client	X-Win 32
WWW-Browser	Internet Explorer 9, Mozilla Firefox

RECHNER	GRAFIK-PC GWDG-B100
Betriebssystem	Windows 7 Enterprise 64 Bit
Grafik	Adobe Creative Suite 6 Design Standard (inkl. Illustrator, InDesign und Photoshop), CorelDRAW Graphics Suite X6, IrfanView
Office	Adobe Acrobat Professional 9, Microsoft Office 2010 (inkl. Access, Excel, InfoPath, OneNote, Outlook, PowerPoint, Publisher, SharePoint, Workspace und Word), OpenOffice 3.2 (inkl. OpenOffice Base, Calc, Draw, Impress, Math und Writer)
SSH-Client	X-Win 32
WWW-Browser	Internet Explorer 9, Mozilla Firefox
Sonstiges	WinCDEmu (bindet ISO-Dateien als virtuelles CD-Laufwerk ein)

RECHNER	OFFICE-PCS GWDG-B101, B102 UND B103
Betriebssystem	Windows 7 Enterprise 64 Bit
Grafik	IrfanView
Office	Adobe Acrobat Professional 9, Microsoft Office 2010 (inkl. Access, Excel, InfoPath, OneNote, Outlook, PowerPoint, Publisher, SharePoint, Workspace und Word), OpenOffice 3.2 (inkl. OpenOffice Base, Calc, Draw, Impress, Math und Writer)
SSH-Client	X-Win 32
WWW-Browser	Internet Explorer 9, Mozilla Firefox

RECHNER	SCANNER-PC GWDG-W7-B01
Betriebssystem	Windows 7 Enterprise 64 Bit
GIS	ArcGIS 10
Grafik	Adobe Creative Suite 5 Design Standard (inkl. Illustrator, InDesign und Photoshop), CorelDRAW Graphics Suite X5, IrfanView, Ghostscript 9.0, Google Earth
Office	Adobe Acrobat Professional 9, Microsoft Office 2010 (inkl. Access, Excel, InfoPath, OneNote, Outlook, PowerPoint, Publisher, SharePoint, Workspace und Word), OpenOffice 3.2 (inkl. OpenOffice Base, Calc, Draw, Impress, Math und Writer)
Scan-Software	EPSON Scan
SSH-Client	X-Win 32
WWW-Browser	Internet Explorer 9, Mozilla Firefox
Peripherie	EPSON Expression 10000LX A3+-Scanner mit Durchlichteinheit

RECHNER	SCANNER-PC GWDG-W7-B02
Betriebssystem	Windows 7 Enterprise 32 Bit
GIS	ArcGIS 10
Grafik	Adobe Creative Suite 4 Design Standard (inkl. Illustrator, InDesign und Photoshop), IrfanView
Office	Adobe Acrobat Professional 9, Microsoft Office 2010 (inkl. Access, Excel, InfoPath, OneNote, Outlook, PowerPoint, Publisher, SharePoint, Workspace und Word), OpenOffice 3.2 (inkl. OpenOffice Base, Calc, Draw, Impress, Math und Writer)
Scan-Software	Nikon Scan 4
SSH-Client	X-Win 32
WWW-Browser	Internet Explorer 9, Mozilla Firefox
Peripherie	Nikon LS-4000 ED Filmscanner zum Scannen von Dias und Negativen im Kleinbildformat

Weiterer Ausbau des Leihrechnerpools der GWDG

Text und Kontakt:
Sven Rosenfeld
sven.rosenfeld@gwdg.de
0551 201-1833

Seit Kurzem steht allen unseren Kunden der neue erweiterte Leihrechnerpool zur Verfügung. Neue Leih-PCs können hier mit vorkonfiguriertem Windows-Betriebssystem und Office-Anwendungen kurzfristig und für eine begrenzte Dauer ausgeliehen werden.

Die GWDG hat aufgrund vermehrter Anfragen nach Leihrechnern und dem erhöhten Bedarf in den Instituten reagiert und den Bestand ihres Leihrechnerpools weiter ausgebaut bzw. durch neu beschaffte Geräte ergänzt. Dieses Angebot erweitert somit den Verleih von Arbeitsplatzrechnern als Dienstleistung für alle Institutsmitarbeiter der Max-Planck-Gesellschaft am Standort Göttingen sowie alle Institutsmitarbeiter und Studierenden der Universität Göttingen.

Liegt eine Störung an einem Arbeitsplatzrechner vor, die es erforderlich macht, dass der Rechner repariert werden muss und vor Ort kein Ersatz vorhanden ist, oder werden kurzzeitig Arbeitsplatzrechner für Veranstaltungen oder Projekte benötigt, so kann die GWDG für eine kurze Leihdauer fertig konfigurierte Windows-Arbeitsplatzrechner zur Verfügung stellen.

Ein solcher Leihrechner ist Mitglied im Active Directory und hat die Softwareausstattung eines Standard-Windows-Arbeitsplatzrechners sowie eine komplette Ausstattung von Peripheriegeräten (Bildschirm, Tastatur, Maus und Netzwerkkabel).

Nach Einstellung der Internet-Adresse (IP-Adresse) vor Ort ist der Institutsmitarbeiter oder Studierende mit dem Leih-PC sofort arbeitsfähig, wenn er bereits Teilnehmer am Active Directory ist, seine E-Mail mit MS Outlook über den Exchange-Server abgewickelt wird und er seine Daten auf dem bereitgestellten persönlichem Netzlaufwerk der GWDG gespeichert hat.

Für Anfragen zu den Leihrechnern wenden Sie sich bitte per E-Mail (*support@gwdg.de*) an die Service-Hotline der GWDG. Wir beraten Sie gerne zum effizienten Einsatz von Leihrechnern und stellen Ihnen diese dann zur Verfügung. Weitere Informationen

zu diesem Thema finden Sie unter *http://www.gwdg.de/index.php?id=81*.

iOS 6 für iPhone und iPad

Text und Kontakt:
Michael Reimann
michael.reimann@gwdg.de

Apple hat am 19. September 2012 für seine mobilen Geräte iPad (2. und 3. Generation), iPhone (3GS, 4 und 4S) und iPod Touch (4. Generation) das Betriebssystem-Update auf iOS 6 bereitgestellt. Damit beginnt eine Reihe interessanter und innovativer Neuvorstellungen im mobilen Bereich. So wird auch Google vermutlich Ende Oktober mit Android 4.2 (Key Lime Pie) eine neue Version seines mobilen Betriebssystems veröffentlichen und der Marktstart für Microsoft Windows Phone 8 zum gleichen Zeitpunkt steht ja schon seit Längerem fest.
iOS 6 beschert seinen Anwendern über 200 neue Funktionen, von denen die Interessantesten hier kurz vorgestellt werden sollen.

NEUE KARTENANWENDUNG

Nachdem bislang Google für die Kartenanwendung in iOS in Form einer separaten App gesorgt hatte, ersetzt nun Apple diese durch eine eigene Lösung. In Zusammenarbeit mit anderen Kartenspezialisten wie beispielsweise TomTom wird neues Kartenmaterial mit integrierter Turn-by-Turn-Navigation (nur ab iPhone 4S, ab iPad 2 und iPod touch 5. Gen.) geboten. Ein Vorteil ist hierbei, dass die Karten nicht mehr aus Einzelbildern zusammengesetzt werden, sondern vektorbasiert aufgebaut sind, was eine flüssigere Darstellung wie beispielsweise bei der Zoom-Funktion gewährleistet. Hinzu kommt mit „FlyOver“ eine neue beeindruckende 3D-Ansicht, die sich allerdings bislang nur auf wenige Großstädte beschränkt (in Deutschland derzeit nur für Berlin und München). Die integrierte sprachgesteuerte geführte Navigation (Turn-by-Turn-Navigation) bietet auch Zugriff auf aktuelle Verkehrsinformationen und übertrifft damit Googles bisherige Lösung. Zwar bietet Google diesen erweiterten Leistungsumfang inzwischen auch für seine Kartenanwendung, allerdings bislang nur für die Android-Geräte. Nutzt der Anwender die Navigationslösung von Apple, muss er daran denken, dass hier stets eine bestehende Internet-Verbindung vorausgesetzt wird, was besonders für Fahrten ins Ausland wegen dort drohender Roaming-Kosten bedeutsam sein dürfte. Hier sind weiterhin Anwendungen wie die von Navigon oder TomTom im Vorteil,

weil sie ihr Kartenmaterial offline bereitstellen und lediglich für das Verkehrsinformationssystem eine Online-Verbindung benötigen. So interessant alle diese neuen Funktionen von Apples eigener Kartenlösung auch sein mögen, an der derzeit noch schwankenden Qualität des Kartenmaterials entzündet sich viel Kritik. So werden oftmals falsche Angaben gemacht, Sehenswürdigkeiten falsch markiert oder Routen nicht korrekt berechnet. Das System ist allerdings so ausgelegt, dass sich das Kartenmaterial im Laufe der Zeit verbessert. Wer sich mit dem derzeitigen Zustand dennoch nicht zufrieden geben will, kann übrigens auch weiterhin auf das Kartenmaterial von Google oder sogar auf das von Nokia ausweichen. Dazu ruft man die beiden Webanwendungen „maps.google.com" und „maps.nokia.com" in Safari auf und legt diese auf den Homescreen, indem die „Teilen"-Schaltfläche aktiviert und der Eintrag „Zum Home-Bildschirm" gewählt wird.

SIRI

Das mit dem iPhone 4S eingeführte Sprachassistenzsystem „Siri" kommt mit iOS 6 nun auch auf das neue iPad und ist damit jetzt auf dem iPhone 5 und 4S, iPad 3. Gen. und iPod touch 5. Gen. vertreten. Zudem bietet es einen erweiterten Funktionsumfang, kann u. a. verschiedene Dienste abfragen, Anwendungen starten, Tweets versenden und den Facebook-Status aktualisieren. Leider reicht der Funktionsumfang immer noch nicht an die US-amerikanische Fassung heran.

SAFARI

Geräte wie das iPhone und das iPad werden besonders gerne zum Surfen im Internet eingesetzt. Das zeigt sich besonders anhand einer Statistik von Webtrekk (Webtrekk, Deutsche Webstatistik 3. Quartal 2012), wonach 11,4 % aller Webzugriffe bereits von mobilen Browsern aus erfolgen. Darunter hat der iOS-Browser Safari mit 68 % den größten Anteil, was seine Bedeutung nur noch unterstreicht. Aus diesem Grund erfuhr er auch eine umfassende Überarbeitung. So gibt es jetzt einen neuen Vollbildmodus, der sichtbar wird, sobald man das iPhone quer hält. Besitzt man einen iCloud-Account, lassen sich die neuen „iCloud Tabs" zwischen den iOS-6-Geräten und Macs mit OS X 10.8 (Mountain Lion) nutzen. Eine in Safari auf dem einen Gerät geöffnete Webseite wird damit über die iCloud auf allen anderen Geräten synchronisiert und kann dort weiter gelesen werden. In der Leseliste werden nun nicht mehr nur die Links, sondern zusätzlich die dazugehörigen Webseiten mit gespeichert, um so künftig auch ohne bestehender Internet-Verbindung offline zum Abruf bereit zu stehen. Das schont so manch begrenztes Datenkontingent. Weiterhin besteht in Formularen nun die Möglichkeit, Dateien wie beispielsweise Bilder hochzuladen, ohne Safari dazu verlassen zu müssen. Ein längeres Betätigen der „Zurück"-Schaltfläche zeigt jetzt den Verlauf der bislang besuchten Webseiten an. Und natürlich ist Safari auch schneller geworden, was vorwiegend der verbesserten JavaScript-Leistung geschuldet ist.

MAIL

Auch bei der Mailanwendung wurde die Benutzeroberfläche optimiert. So wird die Aktualisierung nicht mehr durch eine links unten befindliche Schaltfläche angestoßen, sondern durch das Herunterziehen des Mailfensters („pull to refresh"). Um die Mails bestimmter Adressaten von den übrigen Mails hervorzuheben, gibt es nun die neuen VIP-Listen. Dazu genügt ein Klick auf die Mailadresse des Absenders und Aktivierung des Menüeintrags „Zu VIP hinzufügen". Alternativ kann in der Übersicht der Postfächer auf den blauen Pfeil des „VIP"-Eintrags geklickt werden, um dort dann über „VIP hinzufügen" weitere E-Mail-Adressen aus der Liste aller Kontakte zu wählen. Über den Menüeintrag „VIP-Hinweise" landet man schließlich in der Mitteilungszentrale, in der den eintreffenden Mails der VIPs eine besondere Kennzeichnung zugewiesen werden kann. Natürlich kann mit den VIPs auch ein besonderer Klingelton verbunden werden. Erweist sich jedoch nur eine bestimmte E-Mail als wichtig, kann ihr mittels der neuen Funktion „Markieren" ein orangefarbenes Fähnchen zugewiesen werden. In der Liste aller Mails lässt sich die jeweilige Nachricht dadurch schneller wiederfinden. Eine weitere, gerade für den Business-Bereich sinnvolle Neuerung ist die Möglichkeit, Signaturen für jeden Mail-Account einzeln definieren zu können. Dazu wählt man „Einstellungen > Mail, Kontakte, Kalender > Signatur" und entscheidet dort, ob eine Signatur für alle Accounts oder für jeden einzelnen Account eigene Signaturen zugewiesen werden sollen.

DATENSCHUTZ

Nachdem es in der Vergangenheit immer wieder vorkam, dass Anwendungen einen vom Nutzer ungewollten Zugriff auf die Adressdaten ausübten, hat Apple nun mit iOS 6 diese Art von Zugriffe eingeschränkt und bietet dem Anwender über „Einstellungen > Datenschutz" die Möglichkeit, derartige Zugriffe gezielt zu gewähren oder zu verweigern. Zudem fragen Apps nun grundsätzlich nach, ob der Zugriff auf Kontakte, Kalender, Erinnerungen, den Aufenthaltsort (Ortungsdienste) dem Twitter- oder Facebook-Account erlaubt ist. Wer übrigens keinen Wert darauf legt, sein iPhone durch Werbenetzwerke identifizieren zu lassen, kann die mit iOS 6 eingeführte Werbungs-ID in „Einstellungen > Allgemein > Info > Werbung" über den Eintrag „Ad-Tracking beschränken" deaktivieren. Statt wie bislang die IMEI-Nummer wird nun diese spezielle Gerätekennung verwendet, um die Kontrolle über den Einsatz von Tracking-Methoden durch Werbefirmen zu ermöglichen.

TELEFON

Seit längerer Zeit gibt es auch bei der Telefoniefunktion wieder einmal etwas Neues zu verzeichnen. So kann auf eingehende Telefonanrufe nicht mehr nur mit Ablehnung oder Annahme reagiert werden, sondern sie lassen sich nunmehr auf Wunsch mit

einer Textnachricht beantworten. Alternativ dazu ist es jetzt auch möglich, sich eine Erinnerung für einen späteren Rückruf erstellen zu lassen. Es kann sich dabei sogar um eine ortsabhängige Erinnerung handeln, die sich beispielsweise dann bemerkbar macht, wenn ein bestimmter Ort erreicht bzw. verlassen wird.

„NICHT STÖREN"-MODUS

Viele Anwender werden es bislang vermisst haben, das iPhone in einen Betriebszustand versetzen zu können, in dem alle Anrufe und Benachrichtigungen unterdrückt werden, beispielsweise über Nacht oder für eine Präsentation. Dies gelingt nun seit iOS 6 mit dem neuen „Nicht stören"-Modus in „Einstellungen > Nicht stören". In „Einstellungen > Mitteilungen > Nicht stören" lässt sich dieser sogar noch näher eingrenzen, indem eine Zeitspanne festgelegt werden kann, währenddessen sich das iPhone künftig stummschaltet. Anrufe werden in diesem Zeitraum nicht durchgestellt. Auf Wunsch kann jedoch eine ausgewählte Gruppe von Anrufern durchgelassen werden, oder aber auch Anrufer, die es mehrfach hintereinander versucht haben, den Besitzer des Gerätes zu erreichen.

GETEILTER FOTOSTREAM

Über die bereits in iOS 5 integrierte Fotostream-Funktion lassen sich beispielsweise die auf einem iPhone erstellten Fotos auf freigeschaltete Geräte wie iPad oder Mac übertragen. Voraussetzung dafür ist, dass alle Geräte mit der gleichen iCloud-ID verknüpft sind. Was bislang fehlte, war eine gezielte Bereitstellung der Erzeugnisse für andere Nutzer. Dies ist jetzt mit iOS 6 möglich. Über die neue „Teilen"-Schaltfläche lässt sich jetzt unter „Fotostream" ein neuer Fotostream anlegen, zu dem dann die Teilnehmer eingeladen werden können. Auf Wunsch können die Bilder auch auf eine öffentlich erreichbare Webseite abgelegt werden.

FACETIME ÜBER MOBILFUNKNETZ

Apples eigenes Videochat-Verfahren „Facetime" ist nun nicht mehr nur an das WLAN-Netz gebunden, sondern kann jetzt auch über die UMTS-Datennetze genutzt werden. Voraussetzung dafür sind die aktuellen Geräte iPhone 5, 4S und das neue iPad. Weiterhin sollte man seinen eigenen Mobilfunkvertrag daraufhin überprüfen, ob dort überhaupt die Möglichkeit für Voice-over-IP freigeschaltet ist. Meistens bieten die Netzbetreiber hierzulande diese Funktionalität nur in höherpreisigen Tarifen oder als kostenpflichtige Zusatzoption an. Wichtig für Dienste wie „Facetime" und auch den kostenfreien SMS-Ersatz „iMessage" ist, dass sich jetzt endlich iCloud-ID und Telefonnummer verknüpfen lassen. Nur auf diese Weise können eine beispielsweise an die Mobilfunknummer gerichtete iMessage oder ein Facetime-Anruf auch auf dem iPad oder dem Mac entgegengenommen werden.

FACEBOOK

So wie unter iOS 5 der Microblogging-Dienst Twitter direkt in das Betriebssystem verankert wurde, erfolgt nun die systemweite Integration von Facebook. Im Menü „Einstellungen > Facebook" kann man sich mit seinem Facebook-Account anmelden, und vor allem genau festlegen, welche Apps darauf Zugriff haben sollen. Gerade die Vermischung von eigenen Kontakten und Facebook-Adressen wird ja nicht überall geschätzt und kann hier ausgeschlossen werden. Ist das Facebook-Konto eingerichtet, lassen sich über die neu gestaltete „Teilen"-Schaltfläche direkt vom mobilen Gerät aus verschiedene Aktionen starten.

PASSBOOK

Eine Anwendung mit Potenzial könnte die neue „Passbook App" werden, mit der sich Flugtickets, Bord- und Eintrittskarten, Coupons, Mitgliedsausweise oder andere Dokumente digitalisieren und verwalten lassen. Sie dient dann als eine Art intelligente Sammelmappe für derartige Objekte. Anstatt beispielsweise am Check-in-Schalter oder in speziellen Läden erst die geeignete App herauszusuchen, hätte man so die wichtigsten Dokumente sofort griffbereit. Darüber hinaus wertet Passbook auch die aktuelle Geoposition aus. Sobald der Ort erreicht wird, an dem das jeweilige Dokument benötigt wird, erscheint dieses automatisch auf dem Display des iPhones. Man würde dann beispielsweise gleich die entsprechende Buchungsbestätigung direkt auf dem Sperrbildschirm vorfinden, sobald man im Hotel angekommen ist.

WEITERE NEUERUNGEN

Natürlich sind dies längst nicht alle Neuerungen. Zu nennen wäre da vielleicht noch die Möglichkeit, mit Bordmitteln Panorama-Bilder zu erstellen (nur iPhone 5 und 4S, iPod touch 5. Gen.), oder der „Geführte Zugriff", über den sich das iPhone/iPad derart begrenzen lässt, dass beispielsweise nur eine Anwendung und dort auch nur bestimmte Funktionen aufgerufen werden können.

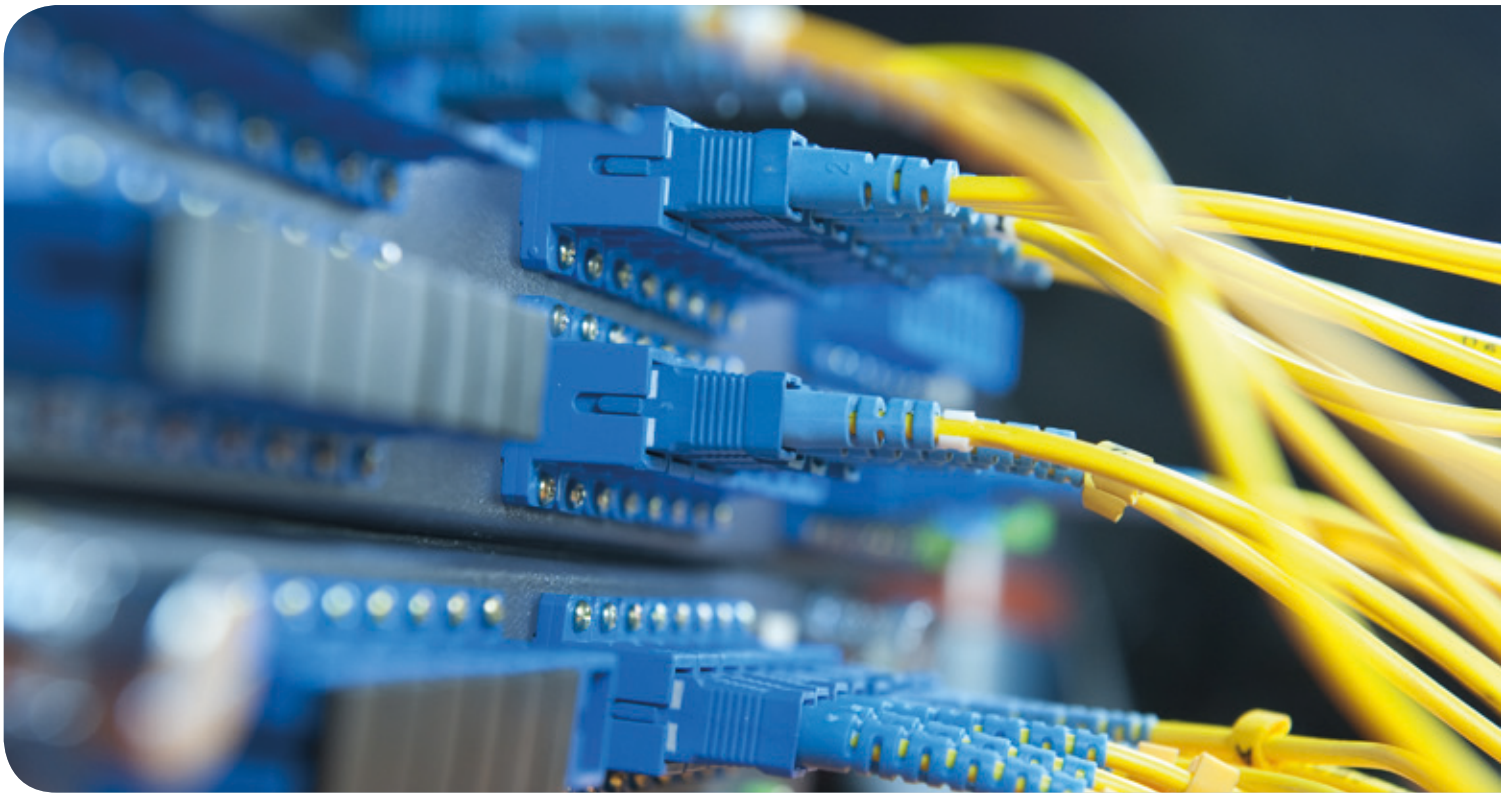
Wer übrigens die Youtube-App aus den vergangenen Betriebssystemversionen vermisst, kann nun eine entsprechend aktualisierte Version aus dem App Store laden. Leider handelt es sich dabei noch um keine Universal App, weswegen man auf dem iPad zu Alternativen wie beispielsweise der kostenlosen App „Jasmine" von Jason Morrissey wird greifen müssen.

INSTALLATION

Das Betriebssystem-Update kann zum einen wie früher üblich über iTunes erfolgen und benötigt dafür die neue iOS-6-kompatible iTunes-Version 10.7. Komfortabler ist aber mittlerweile das Laden über drahtlose Netze, vorzugsweise WLAN, das man über „Einstellungen > Allgemein > Softwareaktualisierung" anstoßen kann. Welchen Weg man auch immer wählt, eine vorherige Sicherung des Gerätes ist auf jeden Fall zu empfehlen.

FAZIT

Die zahlreichen Vorteile von iOS 6, von denen hier ja nur eine kleine Auswahl aufgezeigt werden konnte, lassen ein Update lohnenswert erscheinen, natürlich nur, wenn es die oben geschilderten Hardware-Voraussetzungen zulassen. In diesem Zusammenhang sollte auch nicht unerwähnt bleiben, dass mit iOS 6 auch wieder viele, teils sogar kritische Sicherheitslücken geschlossen wurden. Dieser Aspekt alleine rechtfertigt bereits das Update.



Tipps & Tricks

Verwendung der Netzlaufwerke außerhalb des GÖNET

Falls Sie von außerhalb des GÖNET Ihre Daten erreichen wollen, z. B. von Ihrem PC zu Hause, haben Sie zwei Möglichkeiten: den Zugang über VPN oder den Zugang über einen Terminalserver.

Zugang über VPN

Sie können über einen VPN-Zugang mit Ihren Daten verbunden werden. Der kurze Weg erfolgt über *https://webvpn.gwdg.de*. Hier müssen Sie sich lediglich mit Ihrer GWDG-Benutzerkennung anmelden. Alternativ können Sie einen lokalen VPN-Klienten installieren. Eine detaillierte Beschreibung finden Sie unter *http://www.gwdg.de/index.php?id=303*.

Nachdem die Verbindung mit dem VPN-Client hergestellt ist, können Sie manuell Ihr persönliches Laufwerk verbinden. Weitere Einzelheiten erfahren Sie auch auf unseren Webseiten unter *http://www.gwdg/wlan*.

Zugang über einen Terminalserver

Als zweite Möglichkeit können Sie auch unseren Terminalserver *GWD-WinTS1.top.gwdg.de* verwenden. Wenn Sie sich mit einer Remote-Desktop-Verbindung auf dem Terminalserver mit Ihrem GWDG-Benutzerkonto anmelden, wird automatisch Ihr persönliches Laufwerk verbunden. Bei Bedarf können Sie weitere Laufwerke zusätzlich einbinden. Sofern Sie auf Ihrem Arbeitsplatz im Institut ein gemeinsames Laufwerk (W:) verbunden bekommen, so wird dieses ebenfalls in der Terminalserver-Umgebung automatisch verbunden.

Eine Remote-Desktop-Verbindung (RDP) zu einem Terminalserver herstellen

Um eine Verbindung mit einem Terminalserver herzustellen, starten Sie die „Remotedesktopverbindung“ (RDP), die Sie über „Start > Zubehör > Remotedesktopverbindung“ erreichen. Alternativ können Sie auch über „Start > Ausführen“ den Befehl *mstsc* eingeben und so die RDP-Verbindung starten. Geben Sie im Feld „Computer“ den Namen des Terminalservers (*GWD-WinTS1.top.gwdg.de*) ein und bestätigen Sie mit der „Enter“-Taste. Anschließend erscheint der Anmeldedialog, bei dem Sie sich mit Ihrem GWDG-Benutzerkonto in der Domäne *GWDG* anmelden. Der Server ist mit einem RDP-Clienten (in jedem Windows-Betriebssystem ab Windows 2000 enthalten) zu erreichen. Linux-Benutzer verwenden den RDESKTOP ab Version 1.6.0.

Hast

Kerberos-Authentifizierung von UNIX/Linux-Clients im Active Directory – Teil 3: Die Konfiguration zur „Kerberisierung“ der Clients

Text und Kontakt:
Dr. Konrad Heuer
konrad.heuer@gwdg.de
0551 201-1540
Uwe Gerdes
uwe.gerdes@gwdg.de
0551 201-1514
Thomas Körmer
thomas.koermer@gwdg.de
0551 201-1555

In einer dreiteiligen Artikelserie wird gezeigt, wie man UNIX- und Linux-Systeme an der Active-Directory-Infrastruktur teilhaben lassen kann. Nachdem im Teil 1 in den GWDG-Nachrichten 7/2012 die administrativen Voraussetzungen und im Teil 2 in den GWDG Nachrichten 8/2012 das zweistufige Kerberos-Verfahren erläutert worden sind, geht es im abschließenden dritten Teil um die praktische Einrichtung von UNIX- und Linux-artigen Betriebssystemen. Ziel ist es, eine Kerberos-Anmeldung in die normale Systemanmeldung zu integrieren.

VIRTUELLE TÜRSTEHER – PAM

Fast alle bekannten Distributionen setzen dazu auf die Mitte der 1990er Jahre von Sun Microsystems entwickelten Pluggable Authentication Modules (PAM). Bei diesem System wird ein zentrales Framework zur Verfügung gestellt, auf das Applikationen oder Anmeldedienste wie login oder ssh, aber auch grafische Anmeldeprogramme wie der *Gnome Display Manager* (GDM) über eine API zugreifen können. Der gesamte Anmeldevorgang mit Authentifizierung, Autorisierung und Protokollierung wird von PAM übernommen, die jeweiligen Applikationen bekommen als Information nur eine Rückmeldung, ob die Anmeldung eines Benutzers erfolgreich war oder nicht.

PAM ist modular aufgebaut und kann auf unterschiedliche Authentisierungsverfahren zurückgreifen. Neben PAM-Modulen, die eine herkömmliche UNIX-Authentisierung erlauben (*pam_unix.so*) und eine Passwortüberprüfung von lokalen Accounts in */etc/passwd* und */etc/shadow* durchführen, existieren noch weitere Module. Mit *pam_krb5*.so steht ein Modul zur Verfügung, das Benutzeranmeldungen gegenüber einem Kerberos-KDC prüfen kann.

KERBEROS-CLIENT-INSTALLATION

Für Linux und UNIX gibt es im Wesentlichen zwei freie Kerberos-Implementierungen, die sich sehr ähnlich sind:

- MIT Kerberos
- Heimdal Kerberos

Linux-Systeme verwenden in der Regel die ursprüngliche MIT-Variante, BSD-Systeme setzen dagegen auf die schwedische Alternative Heimdal.

Wie bereits erwähnt (siehe GWDG Nachrichten 7/2012, Teil 1) ist die korrekte Zeitsynchronisation zwischen dem Kerberos-Client und dem Kerberos-KDC Voraussetzung für ein funktionierendes Kerberos-Netzwerk. Sollten die verwendeten Zeitstempel um mehr als fünf Minuten voneinander abweichen, verlieren die verwendeten Tickets ihre Gültigkeit und können nicht mehr verwendet werden.

Eine weitere Bedingung ist die korrekte Namensauflösung von Rechnernamen im DNS; diese sollte vorwärts und rückwärts erfüllbar sein. Kommt es hier zu Fehlern und weicht der aufgelöste Name vom Host-Principal-Eintrag in der */etc/krb5.keytab* ab, werden alle Anmeldungen auf dem Kerberos-Client verworfen.

Als Letztes sollte kontrolliert werden, ob der Kerberos-KDC für den Client über Port 88 erreichbar ist. Am Einfachsten kann das mit *nmap* festgestellt werden:

```
nmap -sT -p T:88  master.top.gwdg.de
Starting Nmap 4.75 ( http://nmap.org ) at 2012-09-10 10:54 CEST
Interesting ports on master.top.gwdg.de (134.76.26.21):
PORT   STATE SERVICE
88/tcp open  kerberos-sec
```

Wurden diese Voraussetzungen erfolgreich überprüft, können die Kerberos-Pakete installiert werden.

Anhand der Beschreibung einer Kerberos-Installation unter Ubuntu soll nun die allgemeine Vorgehensweise erläutert werden.

Abweichungen bei anderen Distributionen werden im Anschluss beschrieben.

UBUNTU 10.04 LTS (LUCID LYNX)

Die Softwareinstallation der benötigten Pakete unter Ubuntu 10.04 ist mit Hilfe von *aptitude* schnell und einfach erledigt. Zusätzlich zur Standarddistribution müssen folgende Pakete nachinstalliert werden:

```
apt-get install krb5-user krb5-doc krb5-config ldap-utils libsasl2-modules-
gssapi-mit libnss-ldap libpam-ldap libpam-krb5
```

Da die Bearbeitung der Konfigurationsdateien im Anschluss manuell erfolgt, können die Dialoge zur Paketkonfiguration übersprungen werden.

Folgende Dateien sollten auf dem System jetzt vorhanden sein:

- */etc/krb5.conf*
- */etc/ldap.conf*
- */etc/samba/smb.conf*
- */etc/nsswitch.conf*

/etc/krb5.conf

Kerberisierte Dienste und Anwendungsprogramme benötigen Informationen über die Kerberos-Infrastruktur, in der sie sich befinden. Darüber gibt als zentrale Konfigurationsdatei die *krb5.conf* Auskunft, die wiederum in mehrere Konfigurationsabschnitte unterteilt ist. Die Defaultparameter werden im Abschnitt *libdefaults* gesetzt. Hier wird dem Client mitgeteilt, zu welchem Kerberos-Realm er gehört. Das kann statisch über den Parameter *default_realm* gesetzt werden, alternativ ist aber auch der Eintrag *dns_lookup_realm=true* möglich. Bei dieser zweiten Variante werden die nötigen Serverinformationen aus dem DNS abgerufen. Im Zonefile des Nameservers befindet sich ein entsprechender TXT-Eintrag mit den passenden Realm-Einträgen. Ein weiterer wichtiger Eintrag bezieht sich auf das Verschlüsselungsverfahren. Aus Kompatibiltätsgründen mit dem Active Directory sollte hier *rc4-hmac-md5* gewählt werden. Alle weiteren Abschnitte (*realms, domain_realms, logging* usw.) sind optional und können nach Bedarf eingefügt werden:

```
[libdefaults]
        default_realm = TOP.GWDG.DE
        default_tkt_enctypes = arcfour-hmac-md5
 [realms]
        TOP.GWDG.DE = {
                kdc = master.top.gwdg.de
                admin_server = master.top.gwdg.de
        }
[domain_realm]
    gwdg.de = GWDG.DE
    .gwdg.de = GWDG.DE
```

/etc/ldap.conf

Für die Verknüpfung der Nutzerdaten aus der Active-Directory-Gesamtstruktur ist die *ldap.conf* zuständig. Neben dem Standardsuchpfad (BASE), LDAP-Server (URI) muss vor allem das Mapping der Windows-Attribute auf die von Linux erwarteten Attribute festgelegt werden. Dieses ist besonders wichtig, da ansonsten der Client die *UID* bzw. *GID* eines Benutzers nicht auflösen kann und den Anmeldevorgang mit einer Fehlermeldung abbricht.

Für die Kerberisierung der Verbindung in das Active Directory müssen sowohl der Pfad zum Ticket-Cache als auch die *SASL*- und *GSSAPI*-Optionen gesetzt werden:

```
BASE        ou=Customers,dc=top,dc=gwdg,dc=de
URI         ldap://master.top.gwdg.de

use_sasl            on
rootuse_sasl        on
sasl_mech           gssapi
krb5_ccname         /var/tmp/krb5cc_0

nss_map_objectclass posixAccount user
nss_map_attribute uid sAMAccountName
nss_map_attribute homeDirectory unixHomeDirectory
nss_map_attribute gecos displayName

nss_initgroups_ignoreusers  (...)
```

Bei Bedarf können hier auch Zugangsbeschränkungen für den Client definiert werden. So ist es denkbar, nur bestimmten Gruppen aus dem Active Directory die Anmeldung zu erlauben. Ein zusätzlicher Eintrag in der *ldap.conf* würde beispielsweise nur den Mitgliedern der Gruppe *ABT100* den Zugriff gewähren:

```
nss_base_passwd ou=GWD,ou=Customers,dc=top,dc=gwdg,dc=de?one?
memberOf=CN=ABT100,OU=-GWD-Groups,OU=GWD,OU=Customers,
DC=top,DC=gwdg,DC=de
```

/etc/samba/smb.conf

Zur Standarddistribution von Ubuntu gehört das Samba-Paket. Sehr nützlich ist das darin enthaltene *net*-Kommando mit seinen Subkommandos, die vor allem zur Verwaltung von Nutzer- und Host-Principals und der *Keytab*-Datei eingesetzt werden können. Da zunächst einmal weitere Samba-Funktionen keine Rolle spielen, ist auch nur eine Minimalkonfiguration (hier als Beispiel für die Domäne *geo.uni-goettingen.de*) notwendig:

```
[global]
        security            = ads
        workgroup           = UG-UG
        realm               = UNI-GOETTINGEN.DE
        kerberos method     = system keytab
```

/etc/nsswitch.conf

Im letzten Schritt wird noch die *nsswitch.conf* angepasst. Dort muss die lokale Auflösung von Benutzern und Gruppen in */etc/passwd* und */etc/group* durch die Einbindung von LDAP (Active Directory) ergänzt werden:

```
passwd:         compat ldap
group:          compat ldap
shadow:         compat
hosts:          files mdns4_minimal [NOTFOUND=return] dns mdns4
networks:   files
protocols:  db files
services:       db files
ethers:         db files
rpc:            db files
netgroup:   ldap
```

Was ist noch zu tun?

Nach dem Anpassen der Konfigurationsdateien erfolgt nun die Bindung des Clients an das Active Directory. Das wird entweder auf dem Windows-DC mit *ktpass.exe* durchgeführt oder auf der Clientseite mit dem Samba-Kommando *net ads join* (siehe GWDG Nachrichten 7/2012, Teil 1). Bei letzterer Methode kann es beim Join in der Konsole zu Fehlermeldungen kommen, die auf mögliche DNS-Probleme hinweisen. In der Regel können diese Meldungen aber ignoriert werden. Bei einer erfolgreichen Anbindung in das Active Directory sollte in der Shell etwas in dieser Art zu lesen sein:

```
Using short domain name – UG-UG
Joined ‚CLIENT01‘ to realm ‚uni-goettingen.de‘
```

Mit einem initialen *kinit*-Befehl wird nun ein Ticket vom KDC geholt. In der Folge sollte dieser Vorgang aber automatisiert werden. Dafür bietet sich ein Startscript an, das mit dem Kommando *update-rc.d* registriert werden kann.

/etc/init.d/krbrefresh (s. Abb. Beginn rechte Spalte)

Um ganz sicher zu gehen, dass die Tickets regelmäßig erneuert werden, wird in */etc/cron.hourly/* ein Cronjob angelegt, der stündlich das Startscript neu aufruft:

```
#!/bin/bash
/etc/init.d/krbrefresh start
```

Nachdem alle notwendigen Einstellungen für die Benutzeranmeldung konfiguriert sind, müssen nun noch die Homeverzeichnisse der Benutzer eingerichtet werden. Grundsätzlich kommen dafür zwei Optionen in Betracht. Entweder werden die Homeverzeichnisse als zentrale Netzlaufwerke über NFS exportiert bzw. als Samba-Share eingebunden, oder als mögliche Alternative dazu sind auch lokale Homeverzeichnisse denkbar. Dabei ist zu beachten, dass auf dem Client der Pfad zu den Homeverzeichnissen identisch ist mit der Pfadangabe im LDAP-Objekt des Benutzers im Active Directory: Das LDAP-Attribut *UnixHomeDirectory=/usr/users/BENUTZERNAME* setzt also ein lokales Verzeichnis */usr/users/BENUTZERNAME* voraus. Um sich hier ein wenig Handarbeit zu sparen, kann für das automatisierte Anlegen von lokalen Homeverzeichnissen das PAM-Modul pam_mkhomedir.so genutzt werden. Durch Hinzufügen folgender Zeile in */etc/pam.d/common-session* übernimmt das Client-System diese Aufgabe:

```
#! /bin/sh
### BEGIN INIT INFO
# Provides:          Kerberos Ticket Refresh
# Required-Start:    $network
# Required-Stop:     $network
# Default-Start:     2 3 4 5
# Default-Stop:      0 1 6
# Description:       This file should be used to refresh the Kerberos
#                    ticket cache
### END INIT INFO

DESC="Kerberos Ticket Refresh"
KRB5CC="/tmp/krb5cc_0"

case „$1" in
        start)
                /usr/bin/kinit -c $KRB5CC -k host/client01.top.gwdg.de -l 2d
        ;;
        stop)
                /usr/bin/kdestroy -c $KRB5CC
                ;;
        status)
                /usr/bin/klist -c $KRB5CC
                ;;
        *)
                echo „Usage: /etc/init.d/krbrefresh (start|stop|status)" >&2
                exit 1
                ;;
        esac
```

```
session  required                pam_mkhomedir.so
```

Etwas Aufmerksamkeit verlangt auch die Shell, die im Benutzerobjekt festgelegt ist. GWDG-Nutzer bekommen, sofern nichts anderes eingestellt ist, als Standard-Shell die Kornshell zugewiesen. Diese muss natürlich auch auf dem Client vorhanden sein, andernfalls hätte das auch hier Fehler zur Folge.

Damit ist jetzt die gesamte Konfiguration abgeschlossen. Active-Directory-Nutzer können sich nun auf einem Linux-System unter Verwendung ihrer AD-Account-Daten anmelden. Allerdings dürfen bei der Anmeldung nur die kurzen Benutzernamen (d. h. *lmuelle* und nicht *gwdg\lmuelle*) verwendet werden, da *nss_ldap* und *pam_krb5* mit der unter Windows üblichen Schreibweise *gwdg\Benutzername* nicht umgehen können.

UBUNTU 11.04 LTS

Mit der Version 11.04 (Natty Narwhal) hat Ubuntu den Display-Manager gewechselt. Statt *gdm* wird nun *lightdm* verwendet. Damit steht eine übergreifende Lösung für alle Desktopumgebungen (Gnome, KDE, LXDE usw.) zur Verfügung. Was allerdings im Startbildschirm fehlt, ist die Option „Andere Benutzer" für die Anmeldung im Active Directory. Durch Hinzufügen der folgenden Zeile in der Datei */etc/lightdm/lightdm.conf* kann dieses Problem aber gelöst werden. Danach steht ein entsprechender Anmeldeknopf zur Verfügung:

```
greeter-show-manual-login=true
```

DEBIAN SQUEEZE

Die Kerberos-Einrichtung von Debian-Clientsystemen unterscheidet sich wenig von der Konfiguration unter Ubuntu. Eine marginale Abweichung gibt es bei den *libnss-ldap*- und *libpam-ldap*-Paketen. Hier nutzen Debian-Syteme statt der ldap.conf die libnss-ldap.conf. Syntaktisch und inhaltlich gibt es aber keinen Unterschied zwischen beiden Konfigurationsdateien.

Etwas eleganter ist bei Debian die Erneuerung des Ticketcache gelöst. Statt eines Startscripts wird aus den Debian-Paketquellen kstart installiert (*apt-get install kstart*). Um kstart beim Systemstart zu initialisieren, genügt ein Einzeiler, der in */etc/inittab* eingefügt wird:

```
KS:2345:respawn:/usr/bin/k5start -U -f /etc/krb5.keytab -K 30 -l 12h
```

Im aktuellen Beispiel ist die Gültigkeitsdauer des Tickets auf zwölf Stunden gesetzt, wobei der im Hintergrund laufende Daemon alle 30 Minuten nachfragt, ob das Ticket noch gültig ist und erneuert werden muss.

FREEBSD

Das Basissystem von FreeBSD 8 beinhaltet bereits eine minimale Installation von Heimdal Kerberos. Damit daraus ein vollwertiger Kerberos-Client wird, müssen noch einige Programmpakete nachinstalliert werden. Traditionell wird dafür auf BSD-Systemen die *Ports Collection* genutzt:

- *nss_ldap: /usr/ports/net/nss_ldap*
- *cyrus-sasl2: /usr/ports/security/cyrus-sasl2*
- *gsasl: /usr/ports/security/gsasl*
- *openldap24-sasl-client: /usr/ports/net/openldap24-sasl-client*
- *samba3: /usr/ports/net/samba3**

Nach dem Wechsel in das gewünschte Verzeichnis wird mit *make install clean* das entsprechende Programmpaket gebaut.

Auch unter FreeBSD gibt es wenig Abweichungen bei der Kerberos-Einrichtung. Etwas anders werden die PAM-Module konfiguriert, eine Anpassung benötigt */etc/pam.d/system*:

/etc/pam.d/system

```
auth        sufficient  pam_opie.so          no_warn no_fake_prompts
auth        requisite   pam_opieaccess.so    no_warn allow_local
auth        sufficient  pam_krb5.so          no_warn try_first_pass
auth        required    pam_unix.so          no_warn try_first_pass nullok
account     required    pam_krb5.so
account     required    pam_login_access.so
account     required    pam_unix.so
session     required    pam_lastlog.so       no_fail
password    required    pam_unix.so          no_warn try_first_pass
```

Da in der Ports Collection *kstart* fehlt, um den Ticketcache regelmäßig zu erneuern, sollten entsprechende *kinit*-Befehle im Crontab eingetragen werden:

/var/cron/tabs/root

```
@reboot /usr/bin/kinit -k -c /var/run/ldap_cc host/client01.top.gwdg.de > /dev/null 2>&1
@hourly /usr/bin/kinit -k -c /var/run/ldap_cc host/client01.top.gwdg.de > /dev/null 2>&1
```

Fehlersuche – Wenn keine Anmeldung möglich ist

Anhand einer kleinen Checkliste sollten zunächst einmal grundlegende Dinge wie Zeitsynchronisation und DNS-Einträge überprüft werden. Erfahrungsgemäß sind das die beiden häufigsten Fehlerquellen. Etwas vielfältiger gestaltet sich danach die Überprüfung der Kerberos-Client-Funktionalität. Hier stehen verschiedene Werkzeuge zur Verfügung.

Mit *klist* (ohne weitere Befehlsparameter) wird der Ticketcache des aktuell angemeldeten Benutzers ausgelesen. Ist der Ticketcache leer, sollte versucht werden, mit *kinit* (z. B. *kinit lmuelle@TOP.GWDG.DE*) ein neues Ticket vom Kerberos-Server zu beziehen. Tickets und Verschlüsselungsverfahren, die in der *Keytab*-Datei liegen, lassen sich mit *klist -e -k -t /etc/krb5.keytab* anzeigen. Zur Erinnerung, die verwendeten Verschlüsselungsalgorithmen müssen sowohl der Client als auch der Server unterstützen. Hilfreich kann unter Umständen auch das Löschen des Ticketcaches imt *kdestroy* sein; ungültige oder beschädigte Tickets lassen sich so sicher vom System entfernen. Ist an dieser Stelle kein Weiterkommen möglich, sollte die Fehlersuche mit den *net*-Kommando des Samba-Pakets fortgesetzt werden. *net ads testjoin* überprüft die erfolgreiche Bindung des Maschinenaccounts an das AD, gegebenfalls muss der Client auch nur das Maschinenpasswort über *net ads changetrustpw -U Administrator* neu aushandeln. Ist die *Keytab*-Datei beschädigt oder ungültig, hilft ein *net ads unjoin -U Administrator* mit anschließendem *net ads join -U Administrator* möglicherweise weiter; die *Keytab*-Datei wird dann neu geschrieben.

LITERATUR

- Kerberos – Single Sign-on in gemischten Linux/Windows-Umgebungen von Mark Pröhl (dpunkt.verlag)
- FreeBSD-Handbuch: *http://www.freebsd.org/doc/de/books/handbook/*
- Debian-Installationsanleitung: *http://www.rjsystems.nl/en/2100-d6-kerberos-openldap-client.php*
- Diverse Ubuntu-Dokumentationen und Foren

Erste Nacht des Wissens in Göttingen am 24. November 2012

Text und Kontakt:
Dr. Thomas Otto
thomas.otto@gwdg.de
0551 201-1828

Premiere – Auch in Göttingen wird es, ähnlich wie schon in einigen anderen Städten bereits erfolgreich etabliert, erstmalig eine Nacht des Wissens geben. Hierzu laden die Universität und viele außeruniversitäre Forschungseinrichtungen – darunter auch die GWDG – gemeinsam ein.

MEHR ALS 200 VERANSTALTUNGEN AN ÜBER 20 STANDORTEN

Wissensdurstig? Entdecker? Experimentierfreudig? Nachtschwärmer? Aufgeschlossen für Neues? Dann sind Sie am 24. November von 17:00 bis 24:00 Uhr bei der ersten Nacht des Wissens genau richtig. Einrichtungen in ganz Göttingen öffnen an diesem Tag ihre Türen für Besucherinnen und Besucher und ermöglichen einen interessanten Blick hinter die Kulissen. Die Nacht des Wissens eröffnet Perspektiven auf aktuelle Fragestellungen und Erkenntnisse am Wissenschaftsstandort Göttingen, die der Öffentlichkeit sonst nicht ohne weiteres zugänglich sind. Egal ob Sie naturwissenschaftlich, philosophisch oder kunstwissenschaftlich interessiert sind – an diesem Tag können Sie Wissenschaft in ihren verschiedensten Facetten kennenlernen. In mehr als 200 Veranstaltungen an über 20 Standorten in ganz Göttingen machen die teilnehmenden Einrichtungen Forschung für alle Alters- und Interessengruppen verständlich und erlebbar: Science Slams, Vorträge, Mitmachaktionen, Führungen, Workshops, Filme und Experimente.

Neben den großen Veranstaltungsorten Zentrales Hörsaalgebäude, Fakultäten für Physik und Geologie auf dem Universitäts-Nordcampus, Universitätsklinikum, Niedersächsische Staats- und Universitätsbibliothek und Deutsches Zentrum für Luft- und Raumfahrt finden Aktionen auch an vielen weiteren Einrichtungen des Wissenschaftsstandortes Göttingen statt. Damit die Besucher einfach und bequem von einem Veranstaltungsort zum nächsten kommen, wird die ganze Nacht ein kostenloser Bus-Shuttle im Einsatz sein. Auf dem Nordcampus sowie im Parkhaus Goßlerstraße stehen zudem kostenlose Parkplätze zur Verfügung. Der Eintritt zu allen Veranstaltungen der Nacht des Wissens ist frei.

GWDG-PRÄSENTATION „CLOUD-DIENSTE FÜR DIE WISSENSCHAFT“

Auch die GWDG ist bei der ersten Nacht des Wissens mit der Präsentation „Cloud-Dienste für die Wissenschaft“ dabei, die im Foyer der Fakultät für Physik, Friedrich-Hund-Platz 1, stattfindet – zusammen mit Aktionen des Zentrums für Angewandte Informatik. Was sind eigentlich Cloud-Dienste? Wie bekomme ich Zugang zur Cloud? Sind meine Daten in der Cloud sicher? Diese und andere Fragen beantworten Mitarbeiter der GWDG, um Besuchern der Nacht des Wissens diesen immer populärer werdenden Dienst mit Blick auf dessen wissenschaftliche Nutzung nahe zu bringen. Abgerundet wird der Programmpunkt durch Demonstrationen und die Möglichkeit, Cloud-Dienste praktisch zu nutzen.

Weitere Informationen zur Nacht des Wissens finden Sie unter *http://www.ndw.uni-goettingen.de*.

Personalia

NEUER MITARBEITER DR. SIAMAK AZODOLMOLKY

Seit dem 15. September 2012 verstärkt Herr Dr. Siamak Azodolmolky die Arbeitsgruppe „eScience“ (AG E) als wissenschaftlicher Mitarbeiter. Er hat in Teheran Computer Engineering und Computer Architecture studiert. Im Anschluss an Tätigkeiten in der Industrie hat Herr Azodolmolky einen zweiten Master an der Carnegie Mellon University, Pittsburgh, sowie eine Promotion an der Universitat Politècnica de Catalunya, Barcelona, abgeschlossen. Er hat über 50 Konferenzbeiträge, Zeitschriftenartikel und Buchkapitel veröffentlicht und als Wissenschaftler für eine Reihe von europäischen Projekten (u. a. DICONET, BONE, OFELIA und FIBRE) im 7. Rahmenprogramm gearbeitet. Bei der GWDG wird sich Herr Azodolmolky u. a. mit Datenmanagement, Software-defined Networks und Cloud Computing befassen. Zudem wird er in der Lehre tätig sein. Er ist per E-Mail unter *siamak.azodolmolky@gwdg.de* und telefonisch unter 0551 39-20362 erreichbar. Seine persönliche Webseite findet sich unter *http://www.gwdg.de/~sazodol.*

Wieder

NEUER MITARBEITER STEFFEN KLEMER

Seit dem 1. Oktober 2012 verstärkt Herr Steffen Klemer die Netzwerkgruppe der Arbeitsgruppe „Basisdienste und Organisation“ (AG O). Er wird Herrn Kai-Uwe Mather während dessen Elternzeit vertreten. Herr Klemer hat an der Universität Göttingen Physik studiert und sein Studium mit dem Diplom über ein Thema aus der Kosmologie in diesem Sommer erfolgreich abgeschlossen. Seine umfassenden Netzwerkkenntnisse stammen unter anderem aus der langjährigen Tätigkeit als Netzwerktutor im Studierendenwohnheim Kellnerweg. Er ist per E-Mail unter *steffen.klemer@gwdg.de* und telefonisch unter 39-172361 erreichbar.

Grieger

INFORMATIONEN:
support@gwdg.de
0551 201-1523

November bis Dezember 2012

Kurse

KURS	VORTRAGENDE/R	TERMIN	ANMELDEN BIS	AE
SHAREPOINT-UMGEBUNG IN DER GWDG	Hast, Helmvoigt, Rosenfeld	13.11.2012 9:00 – 12:30 und 13:30 – 15:30 Uhr	06.11.2012	4
EINFÜHRUNG IN DIE STATISTISCHE DATENANALYSE MIT SPSS	Cordes	21.11. – 22.11.2012 9:00 – 12:00 und 13:00 – 15:30 Uhr	14.11.2012	8
ANGEWANDTE STATISTIK MIT SPSS FÜR NUTZER MIT VORKENNTNISSEN	Cordes	04.12. – 05.12.2012 9:00 – 12:00 und 13:00 – 15:30 Uhr	27.11.2012	8
UNIX/LINUX-ARBEITSPLATZRECHNER – INSTALLATION UND ADMINISTRATION	Gerdes, Dr. Heuer, Körmer, Dr. Sippel	10.12. – 11.12.2012 9:15 – 12:00 und 13:30 – 16:00 Uhr	03.12.2012	8
UNIX/LINUX-SERVER – GRUNDLAGEN DER ADMINISTRATION	Gerdes, Dr. Heuer, Körmer, Dr. Sippel	12.12. – 13.12.2012 9:15 – 12:00 und 13:30 – 16:00 Uhr	05.12.2012	8
UNIX/LINUX – SYSTEMSICHERHEIT FÜR ADMINISTRATOREN	Gerdes, Dr. Heuer, Körmer, Dr. Sippel	14.12.2012 9:15 – 12:00 und 13:30 – 15:00 Uhr	07.12.2012	4

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.

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 *support@gwdg.de* mit dem Betreff „Kursanmeldung" erfolgen. Für die schriftliche Anmeldung steht unter *http://www.gwdg.de/antragsformulare* 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 sieben Tage vor Kursbeginn. Sollten nach dem Anmeldeschluss noch Teilnehmerplätze frei sein, sind auch noch kurzfristige Anmeldungen in Absprache mit der Service-Hotline bzw. Information (Tel.: 0551 201-1523, E-Mail: *support@gwdg.de*) möglich.

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.

Rücktritt und Kursausfall
Absagen durch die Teilnehmer oder die zugehörigen Gruppenmanager bzw. Geschäftsführenden Direktoren können bis zu acht 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.

Kursorte
Alle Kurse finden in Räumen der GWDG statt. Der Kursraum und der Vortragsraum der GWDG befinden sich im Turm 5 bzw. 6, UG des Max-Planck- Instituts für biophysikalische Chemie, Am Faßberg 11, 37077 Göttingen. 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/lageplan* zu finden.

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/kurse* zu finden. Anfragen zu den Kursen können an die Service-Hotline bzw. Information per Telefon unter der Nummer 0551 201-1523 oder per E-Mail an die Adresse *support@gwdg.de* gerichtet werden.


GWDG
Gesellschaft für wissenschaftliche
Datenverarbeitung mbH Göttingen