GWDG
Nachrichten

für die Benutzerinnen und Benutzer des Rechenzentrums

GWDG
Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

Ausgabe 7/2012

Chrome im mobilen Einsatz

Internet-Protokoll IPv6

Authentifizierung mit Kerberos

Inhalt

IMPRESSUM

GWDG-Nachrichten für die Benutzerinnen und Benutzer des Rechenzentrums
ISSN 0940-4686
35. Jahrgang, Ausgabe 7/2012 **Erscheinungsweise: monatlich**
www.gwdg.de/gwdg-nr **Auflage: 500**

Titelfoto: Switch in einem Verteilerschrank im GWDG-Maschinenraum

Herausgeber:	**Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen**		
	Am Faßberg 11		
	37077 Göttingen	**Tel.: 0551 201-1510**	**Fax: 0551 201-2150**
Redaktion:	**Dr. Thomas Otto**	**Tel.: 0551 201-1828**	**E-Mail: Thomas.Otto@gwdg.de**
Herstellung:	**Maria Geraci**	**Tel.: 0551 201-1804**	**E-Mail: Maria.Geraci@gwdg.de**
Druck:	**GWDG / AG H**	**Tel.: 0551 201-1523**	**E-Mail: printservice@gwdg.de**

Googles Chrome im mobilen Einsatz

Mit den neuesten mobilen Versionen von Googles Browser Chrome lassen sich die auf einem Desktopsystem oder Notebook gewonnenen Surfergebnisse wie geöffnete Webseiten, Browserverläufe und Lesezeichen direkt auf die unter dem Betriebssystem Android oder iOS laufenden Smartphones und Tablets übertragen und dort entsprechend weiternutzen.

Chrome 20 für Desktopsysteme

Für Anwender, die viel im Internet unterwegs sind, ist die Wahl eines schnellen und komfortablen Browsers essentiell wichtig. Neben den bekannten Produkten wie Microsofts Internet Explorer, Mozilla Firefox, Apples Safari und Opera erfreut sich seit 2008 ein neuer Browser wachsender Beliebtheit: Googles Chrome. Während dieser Browser ursprünglich nur für die Windows-Plattform verfügbar war, ist er seit der Version 5 (Mai 2010) für Linux und Mac OS X und seit Kurzem auch für die mobilen Geräte unter Android und iOS erhältlich.

Inzwischen nutzen mehr als 310 Millionen Menschen den Chrome-Browser und schätzen dessen hohe Performance (dank der JavaScript-Engine V8), die einfache, nicht überladene Benutzerschnittstelle mit der komfortablen Omnibox, die gleichzeitig als Adress- wie auch als Suchfeld dient, den Inkognito-Modus, der beim Surfen keine Spuren auf dem Gerät hinterlässt, und natürlich den ständig im Hintergrund laufenden „stillen" Updateprozess. Mit einem Klick auf das Schraubenschlüssel-Symbol und „Über Google Chrome" lässt sich stets herausfinden, ob bereits die aktuelle Version installiert ist, und falls nicht, wird das Update sofort angestoßen. In diesen Aktualisierungsprozess mit integriert ist ein eigenes Flash-Plugin, das ebenfalls ohne Zutun des Anwenders regelmäßig auf dem neuesten Stand gehalten wird. Gerade diese sicherheitskritische Browserkomponente wird von Angreifern immer wieder gerne als Ziel für Attacken genutzt. Aber der Chrome bietet noch weitere interessante Sicherheitsfunktionen, wie beispielsweise die Sandbox-Architektur, die den auf präparierten Webseiten schlummernden Schädlingen einen Durchgriff auf die Systemebene zu unterbinden versucht und Anwendungen (Plugins) isoliert. Der Inkognito-Modus sorgt zudem dafür, dass weder der Browserverlauf noch andere Spuren auf dem Gerät zurückgelassen werden. In der aktuellen Version 20 bietet Chrome weiterhin als interessante Neuerung „Chrome to Mobile" und damit eine weitreichende Unterstützung für Mobilgeräte.

Der aktuelle Chrome-Browser lässt sich unter *https://www.google.com/chrome/* herunterladen.

Chrome für Android

Auf der diesjährigen Entwicklerkonferenz Google I/O hat der Hersteller den bereits seit Februar als Beta-Version für sein Mobilbetriebssystem Android verfügbaren Chrome-Browser nun in der finalen Version veröffentlicht. Dieser setzt allerdings die aktuelle Betriebssystemversion Android 4.0 voraus, die derzeit bei nur ca. 8 % der Geräte aufgespielt sein dürfte. Für die Nachfolgeversion Android 4.1 (Jelly Bean) ist Chrome sogar als Standardbrowser vorgesehen, da er im Vergleich zum aktuellen Android-Browser eine höhere Geschwindigkeit, eine bessere Anpassung für Tablets und die von den Desktopversionen her bekannte Sicherheitsarchitektur bietet. Hinzu kommt ein weiterer Geschwindigkeitsgewinn, weil bei einer Suche die relevanten Ergebnisse bereits im Hintergrund geladen werden (Pre-Loading). Hinsichtlich der Bedienung passt er sich den Smartphones an und lässt sich bequem über Mehrfinger- und Wischgesten steuern. Die Internetsuche kann auch über eine Spracheingabe erfolgen.

Besitzt man einen Google-Account und ist dort angemeldet, dann bieten sich vielfältige Synchronisationsmöglichkeiten zwischen der mobilen und der Desktopversion. Das betrifft offene Browserfenster (Tabs), die bereits besuchten Seiten (Browserhistorie) und natürlich die Lesezeichen. Mit dieser Funktion gelingt es beispielsweise, eine bestimmte Reihenfolge besuchter Webseiten auf dem Desktop später auf einem Android-Gerät noch einmal nachzuvollziehen (z. B. mit der „Zurück"-Schaltfläche). Will man andererseits vom Mobilgerät auf bestimmte Webseiten der Desktopversion zugreifen, lassen sich diese über den Menüpunkt „An-

dere Geräte“ anfordern. Dort können die Seiten auf all den Geräten aufgelistet und abgerufen werden, auf denen ein Chrome-Browser läuft und bei denen man mit seinem eigenen Google-Account angemeldet ist.

Chrome für Android lässt sich kostenlos im Google Play Store unter *https://play.google.com/store/apps/details?id=com.android.chrome* herunterladen.

Chrome to Mobile

Die aktuelle oben besprochene Version 20 von Chrome bietet als Neuerung die Funktion „Chrome to Mobile“: Mit einem Klick auf ein kleines Handy-Symbol, welches ganz rechts in der Adressleiste erscheint, wird die gerade geöffnete Webseite direkt an das dort aufgelistete Android-Gerät gesendet (gepusht), auf Wunsch auch zum Offline-Lesen. Voraussetzung hierfür ist, dass auf dem Android-Gerät Chrome für Android installiert und der Benutzer auf beiden Geräten mit seinem Google-Account angemeldet ist. Falls dies dennoch nicht funktioniert, sollte darüber hinaus überprüft werden, ob die Funktion „Chrome to Mobile“ im Desktop-Browser überhaupt aktiviert ist. Das erreicht man mit der Eingabe des Kommandos *chrome://flags* in der Adresszeile. In der daraufhin erscheinenden Liste sucht man den Eintrag „Chrome to Mobile“ und aktiviert ihn mit Klick auf „Aktivieren“. Auch auf dem Android-Gerät muss unter Chrome im Menü „Einstellungen“ > „eigene Google-Mail-Adresse“ der Eintrag „Chrome to Mobile“ aktiviert sein. Jetzt sollte dem erfolgreichen „Pushen“ der aktuellen Webseite vom Desktop auf das Android-Gerät nichts mehr im Wege stehen.

Chrome für iOS

Zum Ende seiner Entwicklerkonferenz hat Google auch Chrome für das iPhone und das iPad veröffentlicht. Aufgrund der Apple-eigenen Restriktionen bringt hier Chrome nicht seine Browser-Engine (mit Javascript V8) mit, sondern baut auf dem Safari-Kern auf und kann somit nicht von seiner gewohnten Geschwindigkeit profitieren. Interessant ist der Browser aber dennoch besonders für diejenigen Anwender, die auf ihren Desktoprechnern oder Notebooks ebenfalls Google Chrome einsetzen und ein Google-Konto nutzen. Denn so ist es auch hier möglich, geöffnete Tabs, die Browserhistorie, Lesezeichen und andere Daten zwischen einem PC und den mobilen Geräten zu synchronisieren. Der Zugriff vom Mobilgerät auf bestimmte Webseiten der Desktopversion wird auch unter Chrome für iOS über den Menüpunkt „Andere Geräte“ erreicht, den man hier unter der Schaltfläche mit den drei Querstrichen findet. Dazu muss der Anwender im Menüpunkt „In Chrome angemeldet“ mit seinem Google-Konto angemeldet sein. Hier findet sich auch ein Menüeintrag „Chrome to Mobile“, der es, wie schon bei den Android-Geräten, ermöglichen soll, Webseiten vom Desktop auf das iPhone/iPad zu schicken. Für ein vollständiges Funktionieren scheint hier allerdings die im Chrome 20 eingebaute „Chrome to Mobile“-Komponente noch nicht auszureichen, so dass stattdessen eine separate Erweiterung dafür erforderlich ist. Diese lädt man, indem nach einem Klick auf das bereits bekannte Schraubenschlüssel-Symbol über die Menüpunkte „Einstellungen“ und „Erweiterungen“ auf den Link „Weitere Erweiterungen herunterladen“ verzweigt wird. In dem darauf erscheinenden Suchfeld wird „Chrome to Mobile“ eingegeben, und sobald diese Erweiterung in der Liste erscheint, lässt sie sich hinzufügen und damit die Push-Funktion für Webseiten auch für iOS-Geräte über das kleine Handysymbol in der Adressleiste ermöglichen.

Chrome für iOS wird als Universal-App (für iPhone und iPad) geliefert und kann hier kostenlos im App Store heruntergeladen werden: *http://itunes.apple.com/de/app/chrome/id535886823*

Fazit

Als Android-Nutzer bietet die Omnipräsenz von Chrome auf allen Plattformen viele Vorteile. An einem Desktop vorgenommene Internetrecherchen lassen sich so nahtlos auf den mobilen Geräten weiterführen. Dass diese Vorgänge über das eigene Google-Konto laufen, wiegt hier nicht so schwer, da Android ohnehin vorwiegend mit einem Google-Account genutzt wird. Aber auch den Anwendern von iPhone und iPad bietet Chrome dank seiner Synchronisationsfähigkeit interessante Möglichkeiten, die sich auf dem Apple-eigenen Safari-Browser mit Bordmitteln nur unzureichend abbilden lassen.

Reimann

Kontakt:
Michael Reimann
michael.reimann@gwdg.de
0551 201-1826

Das neue Internet-Protokoll IPv6 – Teil 2: IPv6 bei der GWDG und im GÖNET

In der letzten Ausgabe der GWDG-Nachrichten wurde eine mehrteilige Artikelserie gestartet, die sich ausführlich mit dem neuen Internet-Protokoll IPv6 beschäftigen soll. Nachdem im Teil 1 die Grundproblematik, die hinter der Einführung des neuen Protokolls steht, behandelt wurde, wird im Teil 2 nun der aktuelle Stand der IPv6-Einführung bei der GWDG und im GÖNET näher dargestellt. Die in loser Folge geplanten weiteren Teile werden sich u. a. mit den neuen IP-Adressen, Adressvergabeverfahren, Migrationsstrategien, Datenschutz- und Sicherheitsaspekten sowie Mobile IP befassen.

Stand der Einführung

Die GWDG verfügt bereits seit Januar 2001 über ein IPv6-Netz. Genutzt wurde das Netz aber zunächst nicht. Die GWDG und vor allem das Informatik-Institut der Universität Göttingen waren ab 2004 am 6WiN-Projekt beteiligt, das ein IPv6-Netz parallel zum damaligen Wissenschaftsnetz G-WiN des DFN darstellte. 6WiN war aus Sicht der GWDG und der Universität aber ein reines Forschungsprojekt, in dem IPv6-Inseln über Tunnel im „normalen“ Netz miteinander verbunden wurden.

2007 wurde der Tunnelbetrieb ersetzt und IPv6 parallel zum IPv4-Protokoll im Wissenschaftsnetz (damals wie heute das X-WiN als Nachfolger des G-WiN) eingeführt. Auch im GÖNET wurde seit 2007 ein IPv6-Netz betrieben, allerdings nur in eher winzigen Teilbereichen, insbesondere in einem kleinen Testnetz des Informatik-Instituts, später in Testnetzen der GWDG, des Geschäftsbereichs IT der UMG und des Instituts für Mathematik. Produktiv genutzt wurde IPv6 aber lange nicht, auch wenn IPv6 im GÖNET-Backbone eigentlich überall verfügbar ist.

Seit Februar 2012 stehen für die Universität, die UMG und das Studentenwerk Göttingen eigene IPv6-Netze zur Verfügung. Erst seit März 2012 wird in einem Teilnetz der GWDG, nämlich in dem Netz, in dem die Arbeitsplatzrechner der GWDG-Mitarbeiter angeschlossen sind, IPv6 produktiv eingesetzt.

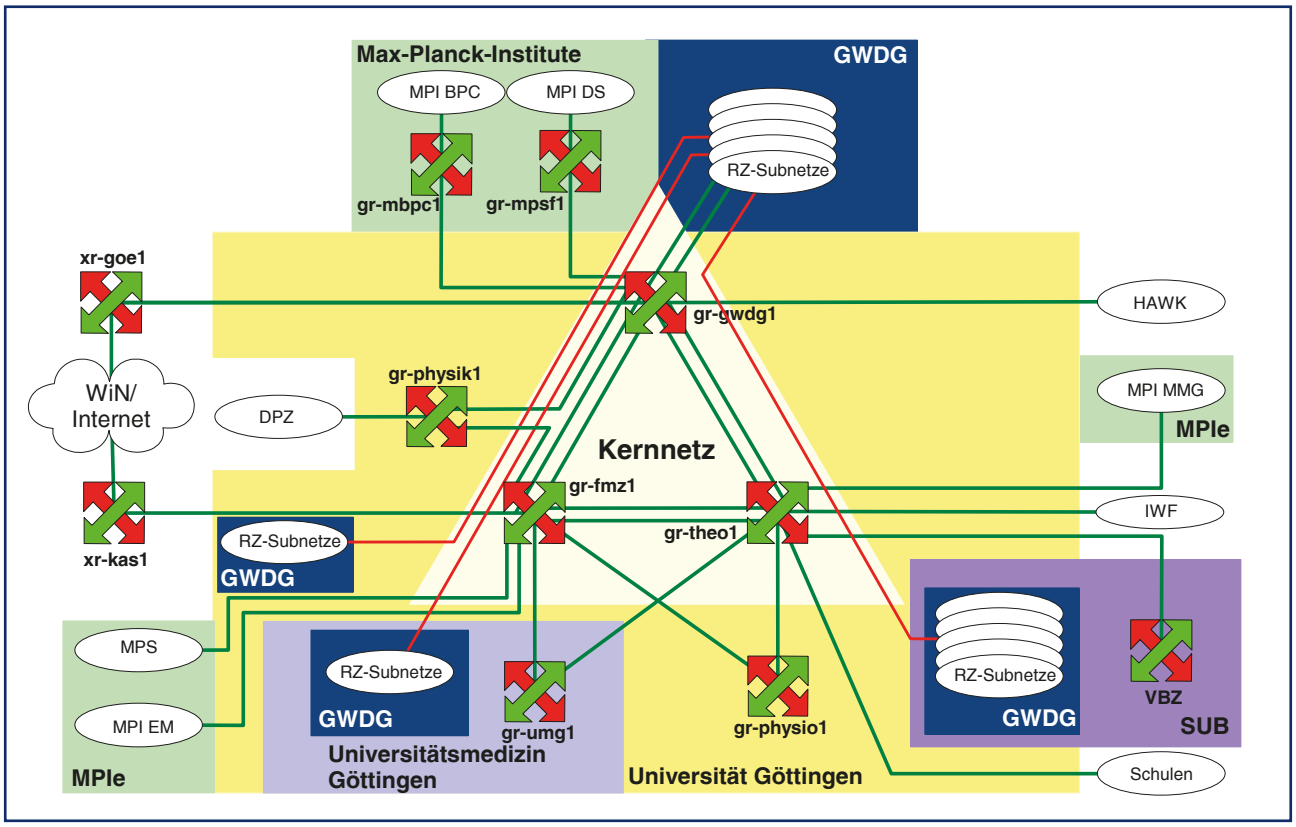
Seit dem 1. Juni 2012 ist auch ein erster öffentlich zugänglicher Server der GWDG über IPv6 erreichbar: der FTP-Server *ftp5.gwdg.de*. In der MPG wird IPv6 bisher kaum eingesetzt. Zurzeit arbeitet eine Projektgruppe an einer einheitlichen IPv6-Adressstruktur für die MPG.

Problematik der Einführung

Nun mögen sich viele vielleicht fragen, warum in elf Jahren im GÖNET bezüglich IPv6 nur so magere Fortschritte erzielt wurden, wenn doch IPv6 angeblich eine wichtige und unverzichtbare Zukunftstechnologie ist. Lange Jahre war der Hauptgrund für den faktischen Verzicht auf IPv6 im GÖNET und in der MPG, dass im Internet kaum Dienste über IPv6 bereitgestellt wurden – und ohne Partner macht der Einsatz von IPv6 keinen Sinn. Der IPv6-Zug hat im Internet erst seit 2011, nachdem der IANA-Pool der IPv4-Adressen verbraucht war, deutlich an Fahrt aufgenommen.

Am World IPv6 Day am 8. Juni 2011 wurde im Internet erstmals in größerem Umfang die Bereitstellung von Diensten, insbesondere Webseiten, über IPv6 getestet, wenn auch an vielen Stellen nur für diesen einen Tag. Nur wenige Dienstanbieter haben nach diesem Tag den IPv6-Betrieb dauerhaft fortgesetzt. Der 6. Juni 2012 wurde von der Internet Society zum World IPv6 Launch Day ausgerufen, der anders als im Jahr zuvor der World IPv6 Day nicht nur zum Testen dienen sollte, sondern zu einer dauerhaften Inbetriebnahme von IPv6-Diensten führen sollte. Tatsächlich sind seitdem viele bedeutende Webseiten über IPv6 erreichbar.

Voraussetzung dafür war natürlich, dass die Internet-Infrastruktur, insbesondere die Internet-Router der Provider, IPv6-fähig ist. Diese Hausaufgaben hatten die Provider tatsächlich im Wesentlichen schon längst erledigt. Das deutsche Forschungsnetz X-WiN z. B. schon seit 2007. Auch im GÖNET-Backbone ist schon seit 2007 IPv6 aktiviert. Trotzdem wird IPv6 im GÖNET praktisch nicht genutzt. Warum? Die Schwachstelle der GÖNET-Infrastruktur sind die Firewall-Systeme im GÖNET. Die derzeitigen, in den GÖNET-Routern (Cisco Catalyst 6500) integrierten Firewall-Systeme stammen aus dem Jahr 2004 und be-



1 *GÖNET-Struktur*

herrschen zwar das IPv6-Protokoll – allerdings nur mit drastischen Leistungseinbußen gegenüber dem Betrieb mit IPv4. Ein Leistungseinbruch um ungefähr eine Größenordnung (d. h. um ca. den Faktor 10) ist aber definitiv niemandem zumutbar.

Für die jetzt schon produktiven Netze der GWDG wurde dieses Firewall-Problem mit Hilfskonstruktionen umgangen. Für eine flächendeckende Einführung im GÖNET sind solche aufwändigen Konstruktionen aber definitiv nicht praktikabel. Die Einführung im GÖNET ist daher solange blockiert, bis die derzeitigen Firewall-Systeme ersetzt sind. Dieser Ersatz ist tatsächlich für 2012/2013 geplant. Nicht nur die Firewall-Systeme, sondern auch die Router des GÖNET-Backbones (s. Abb. 1) haben ein Alter erreicht, in dem ein Ersatz notwendig wird. Die Beschaffung neuer Backbone-Technologie soll 2012 eingeleitet und 2013 abgeschlossen werden. Für die Max-Planck-Institute insgesamt mögen teilweise ähnliche Probleme existieren. Die Situation dürfte hier aber sehr unterschiedlich sein. Für die MPG insgesamt wird ein koordinierter IPv6-Adressraum angestrebt (der IPv4-Adressraum der MPG ist historisch gewachsen und kaum überschaubar). Hier kommen daher neben technischen Problemen auch organisatorische Hürden hinzu, an deren Überwindung derzeit gearbeitet wird.

Mein Rechner, mein Server und IPv6

Der Artikel hat bisher den Blick auf die Netzwerkinfrastruktur gerichtet. Diese ist jedoch nur Mittel zum Zweck, nämlich zur Kommunikation zwischen Anbietern und Nutzern von Diensten im Internet. Diese Infrastruktur ist mit kleinen und hoffentlich bald der Vergangenheit angehörenden Einschränkungen IPv6-fähig. Wie sieht es aber nun mit Servern und Arbeitsplatzrechnern aus?

Die Antwort auf diese Frage ist zum Glück weitgehend beruhigend: Alle aktuellen Versionen der gängigen Betriebssysteme unterstützen problemlos IPv6, ja bei den meisten Systemen ist IPv6 in einer Standardinstallation schon automatisch installiert und aktiviert. Das gilt für die Windows 7 und den Vorgänger Vista (und selbst Windows XP lässt sich IPv6-fähig machen), Mac OS X, Linux-Versionen oder FreeBSD. Windows NT oder Windows 95 kann man allerdings nicht mehr mit IPv6 betreiben – aber wegen fehlender Sicherheitsupdates sollte man diese veralteten Betriebssysteme sowieso ganz und gar nicht mehr ans Netz lassen.

Aus der Vorinstallation von IPv6 resultiert, dass, sobald in einem Netz IPv6 (auf dem Router) aktiviert wird, praktisch alle angeschlossenen Rechner IPv6 in Betrieb nehmen und dank der in den Betriebssystemen in der Standardinstallation hinterlegten Präferenz für IPv6 gegenüber IPv4 sogar bevorzugt nutzen. Die Rechner warten also geradezu nur darauf, endlich loslegen zu können. Voraussetzung für diese automatische Aktivierung von IPv6 ohne weiteres Zutun von Rechneradministratoren ist die bei IPv6 im Standard vorgesehene und üblicherweise aktivierte automatische Konfiguration der IPv6-Adressen und sonstigen Parameter (insbesondere des oder der Router).

Der Wermutstropfen bei dieser weitgehenden Vorbereitung für IPv6 ist allerdings, dass ein absichtlich oder unabsichtlich ins Netz gebrachter, fehlkonfigurierter Router im lokalen Netz ein Sicherheitsproblem darstellt. Gelingt es einem Übeltäter, einen Rechner im Netz als Router zu konfigurieren, der die IPv6-Fähigkeit des Netzes vortäuscht, kann dieser Rechner den Netzbetrieb massiv stören, weil alle Rechner versuchen werden, IPv6 bevorzugt zu nutzen, IPv6-Verbindungen ins Internet aber nicht wirklich vorhanden sind, sondern aller IPv6-Verkehr zu dem falschen Router geführt wird und dort meist enden wird. Der Übeltäter benötigt für einen derartigen Angriff aber den direkten Zugang zum lokalen Netz. Aus dem Internet ist ein solcher Angriff nicht möglich.

Die Betriebssysteme sind also gut auf IPv6 vorbereitet. Wie sieht es mit den Anwendungen aus? Auch hier kann eine beruhigende Antwort gegeben werden: Die Standardanwendungen sind (in aktuellen Versionen) IPv6-fähig. Browser, Mailprogramme oder, etwas betriebssystemnäher, die DNS-Clienten haben keine Probleme mit IPv6. Lediglich Liebhaber älterer Programme könnten sich genötigt sehen, von ihren vertrauten Gefährten Abschied nehmen zu müssen. Gleiches gilt für entsprechende Server-Komponenten. Möglicherweise sind kleinere Konfigurationsmaßnahmen nötig, um IPv6 einzuschalten.

Probleme könnten Spezialanwendungen verursachen, die aus der Natur der Anwendung heraus von IP-Adressen explizit Kenntnis nehmen. Hier könnten Probleme auftauchen, wenn Adressen explizit als Werte von 32 Bit (oder 4 x 1 Byte) Länge einprogrammiert wurden. Solche Anwendungen könnten ohne Überarbeitung in eine IPv6-Welt nicht mehr funktionieren. Ein Beispiel war das alte, selbstentwickelte bzw. über Jahre gewachsene IP-Adressmanagementsystem der GWDG. Andere Adressformate als das gängige IPv4-Format *a.b.c.d* waren darin nicht vorgesehen. Zum Glück ist das System aber schon seit 2009 nicht mehr in Benutzung.

Insgesamt gilt: Je älter, je weniger verbreitet und je spezieller eine Anwendung ist, desto skeptischer sollte man bezüglich der IPv6-Fähigkeit sein.

Mehr Adressen, neue Freiheiten und Strukturen

Die GWDG verfügt für das GÖNET über ein vergleichsweise großes Netz mit immerhin 2^{16} = 65.536 Adressen. Trotzdem musste schon immer mehr oder weniger sparsam mit der Vergabe von Adressen vorgegangen werden. Die Aufteilung des Netzes in Teilnetze geht immer nur durch sukzessive Halbierung, sodass als Größe der Adressbereiche eines Teilnetzes nur Werte 2, 4, 8, 16 usw. in Frage kamen. Zudem konnten die Adressbereiche nur an den entsprechenden Grenzen beginnen (also z. B. ein Bereich mit 64 Adressen nur bei den Endnummern 0, 64, 128 oder 192). Zeitweise mussten sogar alle Teilnetze dieselbe Größe haben. Im Ergebnis hatten alle Teilnetze meist die Größe 256. Davon gab es dann aber nur 256 verschiedene solcher Teilnetze. Damit waren die Möglichkeiten zur Strukturierung des Netzes sehr begrenzt. Letztlich konnte pro Institut oder pro Gebäude meist nur ein Netz mit 256 Adressen zugeordnet werden.

Mit IPv6 sind diese Grenzen weitgehend aufgehoben. Der IPv6-Standard sieht vor, dass für jedes Teilnetz genau 2^{64} = 18.446.744.073.709.551.616 (ca. 18 Trillionen) Adressen zur Verfügung stehen. So viele Adressen werden sicherlich in keinem lokalen Netz jemals benötigt werden. Einrichtungen wie der GWDG oder einer Universität wird typischerweise ein Netz zur Verfügung gestellt, das 2^{16} = 65.536 solcher Teilnetze enthält. Im GÖNET steht der GWDG, der Universität, der UMG und dem Studentenwerk jeweils ein solches Netz zur Verfügung. Jedes MPI wird ebenfalls mindestens ein solches Netz erhalten. Mit IPv6 ist also eine ganz andere, tiefergehende Strukturierung ohne Ad-

ressnöte möglich. Jede Arbeitsgruppe könnte ein oder mehrere Netze erhalten (wobei mehrere Netze z. B. zur weiteren Strukturierung in Sicherheitszonen eingesetzt werden könnten).

Eine Einschränkung trübt diese Freude allerdings: Solange IPv4 und IPv6 parallel genutzt werden und die Netzwerkinfrastruktur keine Trennung in Netze verschiedener Protokolle an einem einzigen Anschluss erlaubt, bremst IPv4 die ganze Neustrukturierung.

Die aktuelle Adressplanung für die Universität sieht pro Fakultät zunächst 256 Teilnetze vor. Der größte Teil der Adressen wird damit immer noch in Reserve gehalten. Warum gerade 256 Teilnetze pro Fakultät eine elegante Gliederung ergeben, wird sich zeigen, nachdem im nächsten Teil der Artikelserie vorgestellt wird, wie IPv6-Adressen aufgebaut sind.

Nächste Schritte

Die GWDG selbst wir in nicht zu ferner Zeit weitere Dienste in IPv6-Netzen anbieten. Die Ausweitung des Diensteangebots ist ein wesentlicher Faktor für die weitere Verbreitung von IPv6, die auch die GWDG vorantreiben möchte. Daher wird die GWDG trotz aller oben aufgeführten Probleme versuchen, in diesem Bereich Fortschritte zu erreichen.

Für Endgeräte im GÖNET wird IPv6 allgemein erst dann angeboten werden, wenn alle Komponenten und insbesondere die Firewall-Systeme IPv6 mit entsprechender Leistungsfähigkeit unterstützen. Dieser Status dürfte leider erst Mitte 2013 erreicht sein. Für Einrichtungen, die ein besonderes, begründetes Interesse an IPv6 haben, wird sich die GWDG bemühen, akzeptable Übergangslösungen zu finden, um IPv6 auch schon vorher bereitstellen zu können.

Beck

Kontakt:
Dr. Holger Beck
holger.beck@gwdg.de
0551 201-1554

Kerberos-Authentifizierung von UNIX/Linux-Clients im Active Directory – Teil 1: Einführung und administrative Voraussetzungen

Das Active Directory von Microsoft ist ein machtvolles Instrument, um große Rechnernetze, wie sie auch am Campus in Göttingen vorliegen, zu verwalten. Aufgebaut ist das Active Directory aus Komponenten, die aus der Open-Source-Welt stammen: Kerberos, LDAP und DNS. In einer dreiteiligen Artikelserie wird gezeigt, wie man UNIX- und Linux-Systeme an der Active-Directory-Infrastruktur teilhaben lassen kann. Im ersten Teil werden nach einer kurzen Einführung die administrativen Voraussetzungen erläutert. In den nächsten Ausgaben der GWDG-Nachrichten folgen der zweite Teil mit einer Beschreibung des zweistufigen Kerberos-Verfahrens und ein dritter Teil mit der Konfiguration zur „Kerberisierung" der Clients für die GWDG-Umgebung.

Überblick

Kerberos ist in der griechischen Mythologie ein dreiköpfiger Hund, der den Eingang zum Reich der Toten bewacht. Für IT-Netzwerkanwendungen übernehmen sogenannte Authentifizierungsdienste diese wichtigen Bewachungsaufgaben. Ein Authentifizierungsdienst, der zum Standard geworden ist, trägt den Namen dieses dreiköpfigen Hundes Kerberos.

Entwickelt wurde dieser Authentifizierungsdienst in den 80er Jahren des 20. Jahrhunderts am Massachusetts Institute of Technologie (MIT) in Boston, USA, im Rahmen eines Forschungsprojektes – dem Athena-Projekt. Die aktuelle Version Kerberos v5 wird allgemein als Kerberos bezeichnet. Ab Windows 2000 wurde von Microsoft der Verzeichnisdienst Active Directory eingeführt und als primärer Authentifizierungsdienst Kerberos v5 in das Active Directory implementiert. Durch die weltweite Verbreitung von Windows Betriebssystemen und Active Directory hat sich schließlich Kerberos als Standard-Authentifizierungsdienst durchgesetzt.

Die GWDG betreibt für ihre Benutzer den Verzeichnisdienst Active Directory (AD). Bestandteil des AD ist der Kerberos-Authentifizierungsdienst, durch den Netz-

werkanwendungen authentifiziert werden. Durch die Funktionalität des Single Sign-on authentisieren sich die Kerberos-Teilnehmer im Netz nur einmal. Anschließend können für diese Sitzung ohne weitere Passworteingabe alle Dienste genutzt werden, die dem Authentifizierungsdienst bekannt gemacht wurden und dem Benutzer bzw. dem Kerberos-Teilnehmer zur Verfügung gestellt werden. Kerberos ist heute Bestandteil aller wichtigen Betriebssysteme und spielt bei der Unterstützung der Netzwerkdienste eine wesentliche Rolle.

Der Kerberos-Authentifizierungsdienst trägt durch die Verwaltung von Identitäten und deren Berechtigungen, auch Identity and Access Management genannt, entscheidend zur Sicherheit in IT-Umgebungen bei. Aber auch IT-Sicherheitsaspekte, wie Integrität und Vertraulichkeit von Benutzerdaten, werden durch Kerberos gewährleistet.

Arbeitsplatzrechner mit einem Windows- oder Mac-OS-X-Betriebssystem können von den AD-Administratoren ohne großen Konfigurationsaufwand in das AD „gehoben" werden und so den Kerberos-Authentifizierungsdienst benutzen. Die benötigten Kerberos-Funktionalitäten sind bereits in den Betriebssystemen implementiert und können menügeführt über grafische Oberflächen konfiguriert werden. Die „Kerberisierung" von UNIX/Linux-Systemen ist etwas aufwändiger und erfordert einige Kenntnisse zur Kerberos-Authentifizierung, da neben einigen administrativen Voraussetzungen etwas Konfigurationsarbeit über die Kommandozeile erforderlich ist.

Dieser Beitrag gibt einen Überblick über die grundlegende Funktionsweise des Kerberos-Authentifizierungsdienstes im AD. Es werden die notwendigen administrativen Voraussetzungen für die Kerberisierung von UNIX/Linux-Betriebssystemen beschrieben. Sie sind für das Funktionieren des Kerberos-Protokolls notwendig und müssen von den Kerberos-Administratoren bereitgestellt werden. Unverzichtbare administrative Voraussetzungen sind

- die KDC-Datenbank, in der die Kerberos-Principals mit ihren Langzeitschlüsseln abgelegt sind,
- Zeitsynchronisation aller Kerberos-Teilnehmer,
- einheitliche Namensauflösung aller Kerberos-Teilnehmer,
- Einrichtung von Principal-Namen für alle Kerberos-Clients und -Services und
- Erzeugung von Client- und Service-Keys.

Anschließend (im Teil 2) wird das zweistufige Kerberos-Verfahren im Überblick beschrieben. Hier wird deutlich, wie Kerberos bei der Authentifizierung gegenüber dem AD mit Tickets und Sitzungsschlüsseln arbeitet. Das zweistufige Verfahren stellt das Single Sign-on zur Verfügung und wird in der Regel verwendet.

Nach dem Überblick über den Ablauf des zweistufigen Kerberos-Verfahrens wird im Teil 3 für zwei weit verbreitete Linux-Betriebssysteme, Ubuntu und Debian, sowie für das UNIX-Betriebssystem FreeBSD die Konfiguration zur Kerberisierung der Clients gezeigt. Abschließend werden einige Werkzeuge vorgestellt, mit denen die Kerberos-Funktionalität der Clients analysiert und verwaltet werden kann.

Administrative Voraussetzungen für eine Kerberos-Authentisierung

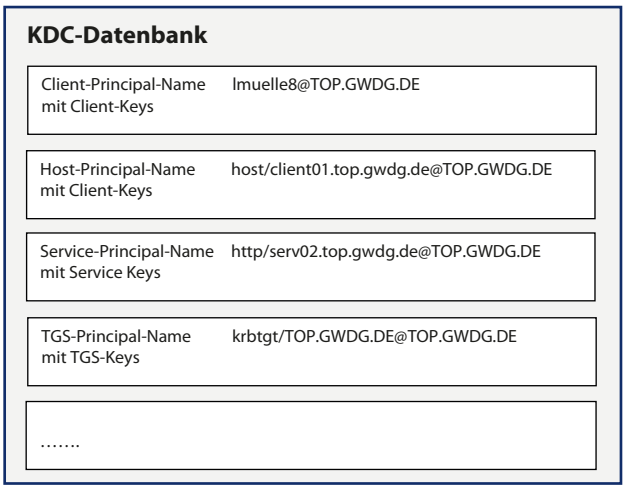
Authentisierung ist allgemein der Nachweis der eigenen Identität. Bei kerberisierten Netzwerkanwendungen müssen beispielsweise Benutzer, Computer oder auch Computerprogramme diesen Nachweis erbringen. Diese Überprüfung der Identität wird als Authentifizierung bezeichnet.

Damit die Kerberos-Authentisierung der UNIX/Linux-Clients und der Zugriff auf kerberisierte Services funktioniert, sind einige administrative Voraussetzungen zu erfüllen. Sie sind für das Funktionieren des Kerberos-Protokolls notwendig und müssen von der Kerberos-Administration bereitgestellt werden.

Die KDC-Datenbank

In der AD-Infrastruktur sorgen Domain Controller (DC) für die Bereitstellung wesentlicher Dienste. U. a. beinhaltet jeder DC einen LDAP-Server, ein Key Distribution Center (KDC) und einen DNS-Server. Das KDC als Kerberos-Server ist eine wesentliche administrative Voraussetzung für die Kerberos-Authentifizierung. In jedem KDC befindet sich eine KDC-Datenbank, in der alle Kerberos-Principals des Realm mit den zugehörigen kryptografischen Langzeitschlüsseln eingetragen sein müssen (siehe Abb. 1). Das KDC kennt so-

mit alle Principals und deren Schlüssel, während die Client -und Service-Principals jeweils nur ihre eigenen Schlüssel kennen. Client- und Service-Principals können Benutzern oder Maschinen zugeordnet werden.



1 *KDC-Datenbank mit allen Kerberos-Principals des Realm und ihren kryptografischen Langzeitschlüsseln*

Zeitsynchronisation aller Kerberos-Teilnehmer

Da Kerberos Zeitstempel für das Erzeugen von Authentikatoren verwendet, müssen unbedingt die Uhrzeiten der beteiligten Systeme synchron sein. Sie sollten nicht mehr als fünf Minuten voneinander abweichen.

Einheitliche Namensauflösung aller Kerberos-Teilnehmer

Die Namensauflösung der Hosts muss auf allen an der Kerberos-Authentifizierung beteiligten Systemen einheitlich funktionieren. Denn DNS-Namen sind ein Bestandteil der Service-Principal-Namen und die Teilnehmer des Authentisierungsvorgangs müssen diese Namen auflösen können.

Principal-Namen für alle Kerberos-Clients- und Services

Jeder Client und jeder Service muss eine Kerberos-Identität in Form eines Principal-Namens besitzen. Denn innerhalb eines Kerberos-Realm werden Clients und Services entsprechend ihrer Funktionalität durch Kerberos-Principals repräsentiert. Ein Client-Principal eines Benutzerobjektes besteht aus dem Benutzernamen und dessen Kerberos-Realm, getrennt durch das @-Zeichen (Beispiel: *lmuelle8@TOP.GWDG.DE*)

Service-Principals repräsentieren Services oder auch Hosts. Bei einem Service-Principal besteht die erste Komponente aus dem Namen des Services und die zweite Komponente aus dem langen DNS-Namen (Fully Qualiified Domain Name, FQDN) der Servermaschine. Nach dem @-Zeichen folgt dann wieder der Realm des Services (Beispiel: *http/serv02.top.gwdg.de@TOP.GWDG.DE*).

Zwei Beispiele sollen verdeutlichen, wie für Clients und Services die jeweiligen Principal-Namen mit den entsprechenden Kerberos-Funktionalitäten zugewiesen werden. Im AD wird ein Objekt durch die Attribute *userPrincipalName* und *sAMAccountName* als Client-Principal beschrieben. Das Attribut *servicePrincipalName* definiert ein Objekt als Service-Principal.

Beim Anlegen eines Benutzerobjektes, beispielsweise *lmuelle8*, mit dem Administrationswerkzeug Active Directory Users and Computers (ADUC) werden u. a. die folgenden Attribute gesetzt. Das Objekt bekommt dadurch als Kerberos-Identität einen Client-Principal-Namen mit der Funktionalität als Client-Principal:

- *userPrincipalName: lmuelle8@TOP.GWDG.DE*
- *servicePrincipalName: nicht gesetzt*
- *sAMAccountName: lmuelle8*

Im zweiten Beispiel soll für ein Maschinenobjekt als Kerberos-Identität ein Service-Principal-Name mit entsprechender Kerberos-Funktionalität erzeugt werden. Beim Anlegen des Objektes, beispielsweise *client01*, im AD werden u. a. diese Attribute gesetzt.

- *userPrincipalName: nicht gesetzt*
- *servicePrincipalName: nicht gesetzt*
- *sAMAccountName: client01$*

Das Maschinenobjekt besitzt damit noch keinen Service-Principal-Namen mit entsprechender Funktionalität. Deshalb muss nun im zweiten Schritt dem Attribut *servicePrincipalName* beispielsweise der Wert *host/client01.top.gwdg.de@TOP.GWDG.DE* zugewiesen werden.

Auf dem DC können dafür der Attribut-Editor des ADUC oder das Kommandozeilentool *setspn.exe* verwendet werden.

```
C:\Users\Administrator>setspn.exe –R client01$
```

Nun hat das Maschinenobjekt die Kerberos-Funktionalität eines Service-Principals.

- *userPrincipalName:* *nicht gesetzt*
- *servicePrincipalName:* *HOST/client01; HOST/client01.top.gwdg.de*
- *sAMAccountName:* *client01$*

Vom Arbeitsplatzrechner *client01* kann abschließend getestet werden, ob die Zuweisung des Service-Principals erfolgreich war.

```
client01> kvno host/client01.top.gwdg.de
```

Für das Anlegen von allgemeinen Service-Principals werden i. d. R. Service-Accounts verwendet. Das sind Benutzerobjekte, denen ein oder mehrere servicePrincipalName-Attribute zugewiesen werden. Über den Aufruf des Kommandozeilentools *setspn.exe –a* werden alle Parameter mit Beispielen für die Zuweisung dieser Attribute bereitgestellt.

Einem Maschinenobjekt kann als Kerberos-Identität auch ein *userPrincipalName* mit entsprechender Client-Funktionalität zugewiesen werden. Dazu können beispielsweise die im folgenden Abschnitt beschriebenen Werkzeuge *ktpass.exe* und *net ads join* verwendet werden.

Client Keys und Service Keys – Erzeugen von Keytab-Dateien

Jeder Kerberos-Client und -Dienst muss jeweils einen oder mehrere kryptografische Langzeitschlüssel mit unterschiedlichen Verschlüsselungsverfahren besitzen. Der Langzeitschlüssel eines Client-Principal wird als Client-Key bezeichnet und der Langzeitschlüssel eines Service-Principal als Service-Key.

Clients als Benutzerobjekte erhalten ihre Client-Keys über das Anwenderpasswort. Aus dem Anwenderpasswort werden mit den string2key-Funktionen die Keys abgeleitet. Für UNIX- und Linux-Systeme als Maschinenobjekte müssen vom Kerberos-Administrator die Keys aus der KDC-Datenbank des DC geholt und in Keytab-Dateien auf dem jeweiligen Client-System hinterlegt werden. Dadurch haben die Clients direkten Zugriff auf ihre Client-Keys. Auch Dienste haben direkten Zugriff auf ihre Service-Keys, die sich in den Keytab-Dateien auf den jeweiligen Systemen befinden. Zusammengefasst haben Keytab-Dateien zwei Funktionen:

- Kerberos-Clients verwenden Keytab-Dateien, damit beim Beziehen initialer Tickets kein Passwort erforderlich ist.
- Bereitstellung der Keys, damit die Kerberos-Teilnehmer ihre Tickets validieren können.

Zur Erzeugung der Keytab-Dateien können vom Kerberos-Administrator verschiedene Werkzeuge eingesetzt werden. Die Verwendung der Tools *ktpass.exe* und *net ads join* sollen im Folgenden beschrieben werden.

1. Erzeugung einer keytab-Datei auf dem Windows-DC mit dem AD-Werkzeug ktpass.exe

Das AD-Werkzeug *ktpass.exe* wird vom Kerberos-Administrator auf dem Windows-DC ausgeführt. Damit *ktpass.exe* eine Keytab-Datei für ein Maschinen-Objekt erstellen kann, muss der AD-Administrator einige Parameter definieren. Die Option *ktpass.exe –help* listet alle Optionen auf, die für die Keytab-Erzeugung zur Verfügung stehen. Im ersten Beispiel ist neben notwendigen Optionen beispielsweise der kryptografische Schlüssel für das Verschlüsselungsverfahren im Netzwerk definiert, der von den Kerberos-Teilnehmern verwendet werden soll. Auch das Passwort wird hier fest vorgegeben.

```
C:\ ktpass.exe /out krb5.keytab /mapuser host/client01.top.gwdg.de /
princ host/client01.top.gwdg.de@TOP.GWDG.DE /crypto AES256-SHA1 /
pass UN+46p45Y9 /ptype KRB5_NT_PRINCIPAL -mapop set +desonly
```

Das zweite Beispiel zeigt eine weitere Möglichkeit, gezielt Optionen bei der Erstellung einer Keytab-Datei zu übergeben.

```
C:\ ktpass.exe /out krb5.keytab /mapuser host/client01.top.gwdg.
de /princ host/client01.top.gwdg.de@TOP.GWDG.DE /crypto all /pass
rndpass /ptype KRB5_NT_PRINCIPAL -mapop set +desonly
```

Die erzeugte keytab-Datei *krb5.keytab* muss anschließend vom DC über einen sicheren Weg auf das zu kerberisierende UNIX/Linux-System kopiert werden und mit den notwendigen Rechten versehen unter */etc* abgelegt werden.

```
client01> chmod 600 etc/krb5.keytab
```

Nach der Erstellung der Keytab-Datei für das gewünschte Maschinenobjekt sind die Kerberos-Attribute wie folgt gesetzt:

- *userPrincipalName:* *host/client01.top.gwdg.de@TOP.GWDG.DE*
- *servicePrincipalName:* *host/client01.top.gwdg.de*
- *sAMAccountName:* *client01$*

Mit den Kommandos *kinit* und *kvno* kann abschließend auf dem UNIX/Linux-System die Keytab-Datei überprüft werden. Das Kommando *kinit* testet den userPrincipalName und das Kommando *kvno* testet die Verfügbarkeit des Service-Principals im AD. Durch die Option des Kommandos *kvno –k* werden auch gleich die enthaltenen Schlüssel in der Keytab geprüft.

```
client01> kinit –k host/client01.top.gwdg.de
client01> kvno –k /etc/krb5.keytab host/client01.top.gwdg.de
```

2. Erzeugung einer keytab-Datei mit dem SAMBA-Werkzeug net ads join

Das SAMBA-Softwarepaket, in dem das SAMBA-Werkzeug *net ads join* enthalten ist, wird mit der Distribution einiger Linux-Systeme wie Ubuntu und Debian mitgeliefert und muss deshalb nicht zusätzlich installiert werden. Für das Betriebssystem FreeBSD ist das SAMBA-Paket nachträglich zu installieren. Um die SAMBA-Werkzeuge nutzen zu können, ist eine Anpassung der SAMBA-Konfigurationsdatei *smb.conf* notwendig.

```
client01> vi /etc/samba/smb.conf
[global]
security = top
workgroup = GWDG
realm = TOP.GWDG.DE
kerberos method = system keytab
```

Nun kann der Kerberos-Administrator auf dem UNIX/Linux-System mit Hilfe von *net ads join* in einem Schritt einen Maschinen-Account auf dem Windows-DC erstellen und eine Keytab-Datei *krb5.keytab* erzeugen, die gleich auf dem Arbeitsplatzrechner unter */etc* ablegt wird.

```
client01> net ads join -U krbadmin createupn = host/client01.top.gwdg.de @TOP.GWDG.DE
```

Folgende Optionen können beim Einrichten eines Maschinen-Accounts hilfreich sein, um im AD-Verzeichnisbaum die Objekte strukturiert abzulegen:

- Mit der Option *–s* kann der DC angegeben werden, der genutzt werden soll.
- Die Option *createcomputer* ermöglicht das gezielte Anlegen des Maschinen-Accounts in eine OU der Domäne.

```
client01> net ads join -U krbadmin -s master.top.gwdg.de createupn = host/client01.top.gwdg.de @TOP.GWDG.DE createcomputer='Test-Kerberos/Computers'
```

Mit den Kommandos *kinit* und *kvno* kann auf dem UNIX/Linux-System schließlich die Keytab-Datei überprüft werden.

```
client01> kinit –k host/client01.top.gwdg.de
client01> kvno –k /etc/krb5.keytab host/client01.top.gwdg.de
```

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

Gerdes, Heuer, Körmer

Kontakt:

Uwe Gerdes
uwe.gerdes@gwdg.de
0551 201-1514

Dr. Konrad Heuer
konrad.heuer@gwdg.de
0551 201-1540

Thomas Körmer
thomas.koermer@gwdg.de
0551 201-1555

Personalia

25-jähriges Dienstjubiläum von Dr. Rainer Bohrer

Nach erfolgreichem Studium der Chemie und der Politikwissenschaften und nach der Promotion mit einem Dissertationsthema zur Chemie der Uranchloride und -bromide hatte Herr **Dr. Rainer Bohrer** 1987 eine Stelle als wissenschaftlicher Mitarbeiter im Gmelin-Institut für Anorganische Chemie angetreten. Dort arbeitete er u. a. an der Spezialdatenbank für Abkürzungen in der Chemie und am Gesamtregister des Handbuchs für anorganische Chemie, für das er später bis zur Schließung des Instituts als Fachredakteur tätig war.

Er kam dann 1998 zur GWDG und hat sich damals schon in der AG 3 mit Bioinformatik-Software und Gensequenzdatenbanken beschäftigt sowie mit den Themen XServer, SSH und PGP. Nach dem Wechsel in die AG A, der sich durch die Restrukturierung der Arbeitsgruppen der GWDG ergab, wurde der Bereich Bioinformatik immer wichtiger. In diesem Bereich gelang es Herrn Bohrer in besonderem Maße das zu schaffen, was zu den Gründungsaufgaben der GWDG zählt, nämlich im IT-Umfeld Synergien zwischen Instituten der Universität und der MPG in Zusammenarbeit mit der GWDG zu schaffen. Das Göttingen Proteomics Forum (*http://www.goeprofo.gwdg.de*), dem Herr Bohrer als Mitglied angehört, ist ein Beleg dafür und wichtiges Netzwerk im Goettingen Research Campus.

Neben seiner IT-Kompetenz, die seine Kunden und Kollegen kennen und schätzen, ist auch seine Sozial-Kompetenz zu betonen: Zehn Jahre Betriebsratstätigkeit, hohe Kommunikationsfähigkeit und die Organisation einiger besonders gut gelungener Betriebsausflüge sprechen dafür.

Wir bedanken uns bei Rainer Bohrer und gratulieren ihm herzlich zum 25-jährigen Dienstjubiläum!

Heise

Zwei neue Hilfskräfte in der AG E

Seit dem 1. Juni 2012 verstärken Herr **Truong Khanh Linh Dang** als wissenschaftliche und Frau **Maria Moloci** als studentische Hilfskraft die Arbeitsgruppe „eScience“ (AG E).

Herr Dang hat an der Ho Chi Minh University of Science in Vietnam sein Studium der Informatik mit dem Bachelorgrad abgeschlossen und absolviert nun an der Universität Göttingen ein Masterstudium in Angewandter Informatik.

Frau Moloci studiert zurzeit an der Universität Göttingen im Bachelorstudiengang Informatik mit dem Anwendungsfach Medizin.

Beide neuen Hilfskräfte werden bei der GWDG an Projekten aus dem Bereich Cloud Computing mitarbeiten.

Sie sind beide telefonisch unter der Nummer 0551 39-20442 und per E-Mail unter *linh.dang@gwdg.de* bzw. *maria.moloci@gwdg.de* erreichbar.

Wieder

Kurse von August bis Dezember 2012

Allgemeine Informationen zum Kursangebot der GWDG

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.

Kurs	Vortragende/r	Termin	Anmeldeschluss	AE
Grundlagen der Bildbearbeitung mit Photoshop	Töpfer	28.08. – 29.08.2012 9:30 – 16:00 Uhr	21.08.2012	8
InDesign – Grundlagen	Töpfer	04.09. – 05.09.2012 9:30 – 16:00 Uhr	27.08.2012	8
Einführung in die Bedienung eines Windows-PCs	Becker, Nolte, Quentin	10.09.2012 9:00 – 12:30 und 13:30 – 15:30 Uhr	03.09.2012	4
Grundkurs UNIX/Linux mit Übungen	Hattenbach	11.09. – 13.09.2012 9:15 – 12:00 und 13:30 – 16:00 Uhr	04.09.2012	12
Installation und Administration eines Windows-Arbeitsplatzrechners	Becker, Nolte, Quentin	17.09.2012 9:00 – 12:30 und 13:30 – 15:30 Uhr	10.09.2012	4
Photoshop für Fortgeschrittene	Töpfer	18.09. – 19.09.2012 9:30 – 16:00 Uhr	11.09.2012	8
Administration von PCs im Active Directory der GWDG	Buck, Hast	25.09.2012 9:00 – 12:30 und 13:30 – 15:30 Uhr	18.09.2012	4
Outlook – E-Mail und Groupware	Helmvoigt	27.09.2012 9:15 – 12:00 und 13:00 – 16:00 Uhr	20.09.2012	4
UNIX für Fortgeschrittene	Dr. Sippel	15.10. – 17.10.2012 9:15 – 12:00 und 13:15 – 15:30 Uhr	08.10.2012	12
Smartphones und Tablets (iPad) für denwissenschaftlichen Einsatz	Reimann	17.10.2012 9:00 – 12:00 und 13:00 – 16:00 Uhr	10.10.2012	4
InDesign – Aufbaukurs	Töpfer	18.10. – 19.10.2012 9:30 – 16:00 Uhr	11.10.2012	8
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