GWDG NACHRICHTEN 03|15

GWDG CrashPlan PROe

Spam und Phishing-E-Mails

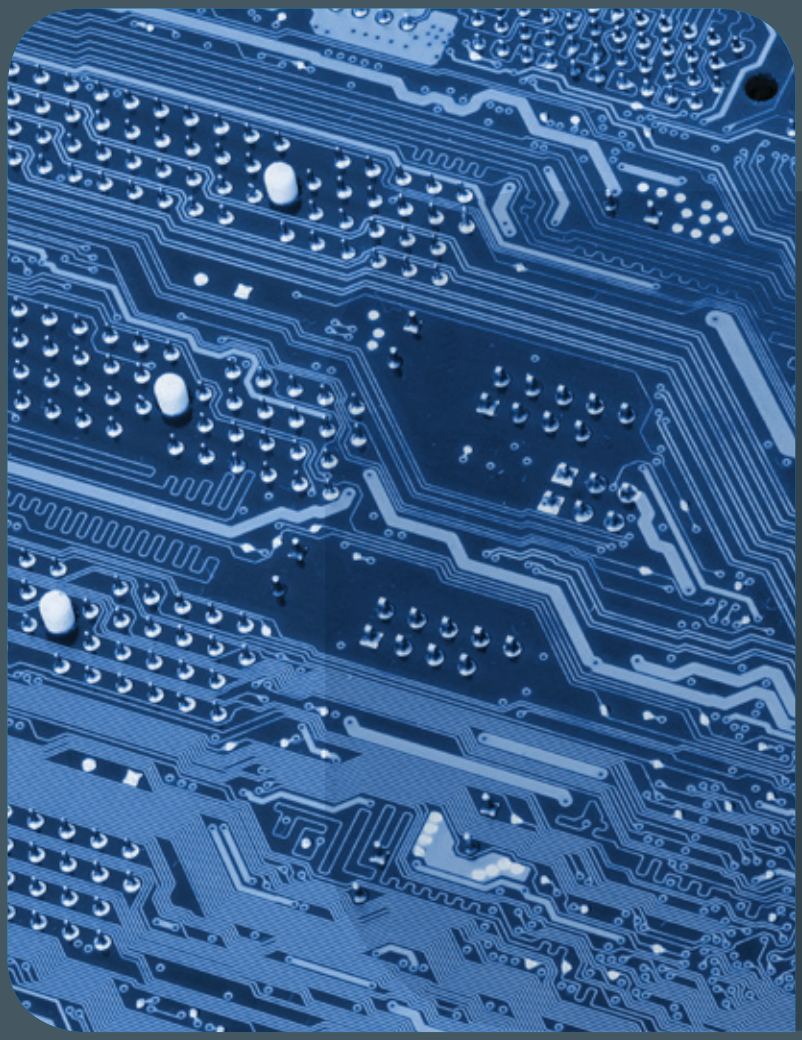
Microsoft-Software

Helium Backup für Android

Debugger gdb

EU-Projekt „Mikelangelo“

ZEITSCHRIFT FÜR DIE KUNDEN DER GWDG



GWDG
NACHRICHTEN

03|15

Inhalt

Impressum

Zeitschrift für die Kunden der GWDG

ISSN 0940-4686
38. Jahrgang
Ausgabe 3/2015

Erscheinungsweise:
monatlich

www.gwdg.de/gwdg-nr

Auflage:
500

Fotos:
@ Mathias Rosenthal - Fotolia.com (1)
@ Foto Zihlmann - Fotolia.com (7)
@ pterwort - Fotolia.com (8
@ Sashkin - Fotolia.com (24)
@ MPIbpc-Medienservice (3, 22, 23)
@ GWDG (2, 25)

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,

die GWDG bietet ihren Kunden schon seit einigen Jahren diverse Cloud-Dienste an, um Alternativen zu kommerziellen Angeboten zu liefern. Die GWDG-Dienste laufen in unseren lokalen Rechenzentren, womit die Daten auf unseren Servern verbleiben und damit nicht in Drittländer oder zu kommerziellen Providern gelangen. Mit dem „GWDG Cloud Server" gibt es seit zwei Jahren ein Angebot für virtuelle Maschinen im Selfservice. Die technische Basis hierfür ist OpenStack mit einer KVM-Virtualisierung, womit eine sehr kostengünstige Umgebung für die Bereitstellung von virtuellen Maschinen möglich ist. Die GWDG betreibt aber nicht nur solche Infrastrukturen, sondern ist über Drittmittelprojekte auch an der innovativen Weiterentwicklung beteiligt. In diesen GWDG-Nachrichten finden Sie einen Bericht über das neue EU-Projekt „Mikelangelo". Hier wird mit mehreren internationalen Partnern an hochperformanter Datenkommunikation über RDAM für die Virtualisierung in OpenStack und in HPC-Batchmanagement gearbeitet. Wir werden in weiteren Ausgaben über dieses sehr interessante Projekt berichten.
Ich wünsche Ihnen viel Freude beim Lesen dieser Ausgabe der GWDG-Nachrichten.

Ramin Yahyapour

GWDG – IT in der Wissenschaft

Neuer Dienst „GWDG CrashPlan PROe“

Text und Kontakt:
Simon Heider
simon.heider@gwdg.de
0551 201-1840

Die Anforderungen an das Backup von Endgeräten haben sich im Laufe der Zeit geändert. Die GWDG reagiert auf diese Entwicklung und bietet nun einen zusätzlichen Dienst im Bereich Backup an. Nach internen Tests und Vergleichen hat sich die GWDG dafür entschieden, ihren Kunden das Produkt „CrashPlan PROe“ anzubieten. Hierfür wurde ein Rahmenvertrag abgeschlossen, der es unseren Kunden – vorerst für drei Jahre – ermöglicht, CrashPlan PROe zu besonders günstigen Konditionen zu lizenzieren. Die maßgeblichen Gründe für „CrashPlan PROe“ sind das Lizenzmodell, das an die Benutzerkonten und nicht an die Endgeräte gekoppelt ist, sowie die einfache, intuitive Installation und Bedienung. Da die Daten mit dem Blowfish-Algorithmus verschlüsselt und ausschließlich bei der GWDG gespeichert werden, sind sie vor dem Zugriff unbefugter Dritter sehr gut geschützt. Die Software ist außerdem mit allen gängigen Betriebssystemen kompatibel (Linux, Mac, Windows und Solaris). Zusätzlich können per Webzugriff die gesicherten Daten sowohl auf dem PC als auch auf mobilen Endgeräten wiederhergestellt werden.

EINLEITUNG

Um dem Umstand Rechnung zu tragen, dass immer mehr unserer Kunden mit dem Laptop von unterwegs arbeiten und dabei ein Maximum an Flexibilität benötigen, bietet die GWDG für Endgeräte einen neuen Backupdienst an: „GWDG CrashPlan PROe“. Hierbei handelt es sich um ein mit allen gängigen Betriebssystemen (Linux, Mac, Windows und Solaris) kompatibles, verschlüsseltes, cloud-basiertes Datenbackup mit Versionierung. Die Entscheidung für dieses Produkt „CrashPlan PROe“ [1] – das „e“ steht für den inhouse-Betrieb bei der GWDG – hat mehrere Gründe:

Zunächst einmal hat das Produkt bei internen Tests im Vergleich zu Mitbewerbern wie z. B. „insync“ [2] am meisten überzeugt. Außerdem ist das Produkt bereits bei mehreren Max-Planck-Instituten im Einsatz und erfreut sich dort großer Nutzerakzeptanz. Auch große Firmen, sowohl aus dem IT-Bereich als auch aus vielen anderen Dienstleistungs- und Industriesparten, setzen auf CrashPlan. Ausschlaggebend war schließlich, dass der deutsche Vertriebspartner, die Firma VNC, in unserem Auftrag gute Konditionen für einen Rahmenvertrag ausgehandelt hat, die wir an unsere Kunden weitergeben können.

CrashPlan PROe wird komplett im Rechenzentrum der GWDG betrieben und durch den Einsatz des offenen Blowfish-Algorithmus von Bruce Schneier [3] und, bei Bedarf, eines zusätzlichen Passwortes, sind Ihre Daten sehr gut vor dem Zugriff durch unbefugte Dritte geschützt. [4] Um im Notfall an die Daten zu kommen, wird den Nutzern empfohlen, den sogenannten Accountschlüssel aus dem Account herauszukopieren und an einem sicheren Ort zu verwahren.

Der Zugriff auf „GWDG CrashPlan PROe“ ist nur aus dem GÖNET oder über VPN möglich. Die Wiederherstellung von Daten kann sowohl mit dem Browser, auch von Mobilgeräten aus, als

New service „GWDG CrashPlan PROe“

Addressing the changes in the field of backup for endusers, GWDG takes action and decided, after internal comparisions and testing, to provide to its customers another offer in the field of backup services – the product CrashPlan PROe. Therefore a frame contract for our customers with the duration of three years was reached / arranged. The leading advantages for our customers are that the licence model where the licences are bound to the user account and not to the device and the easy intuitive setup process for the enduser and its easy administration. As all data is encrypted by using the blowfish-algorithm and stored exclusively at GWDG, the data is protected in a very good way against access by unauthorized third parties. Furthermore, the software is compatible with all popular operating systems (e.g. different flavors of Linux, Mac, Windows and Solaris). In addition data can be restored via a webinterface either on the computer or on the mobile devices.

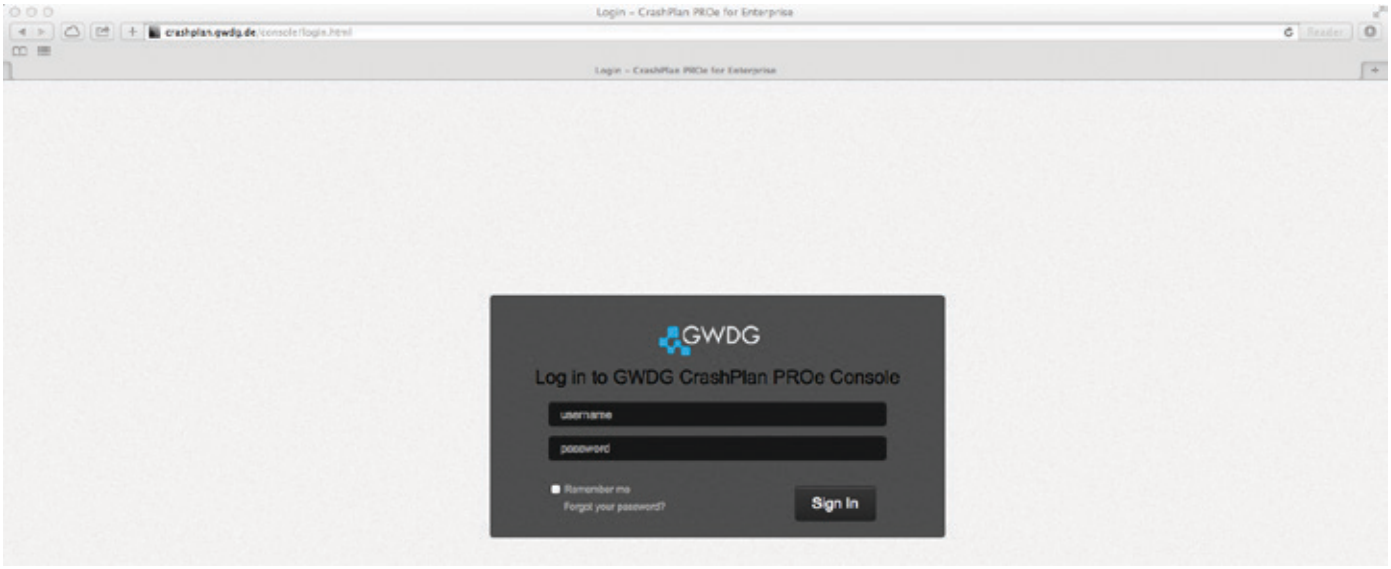


Abb. 1

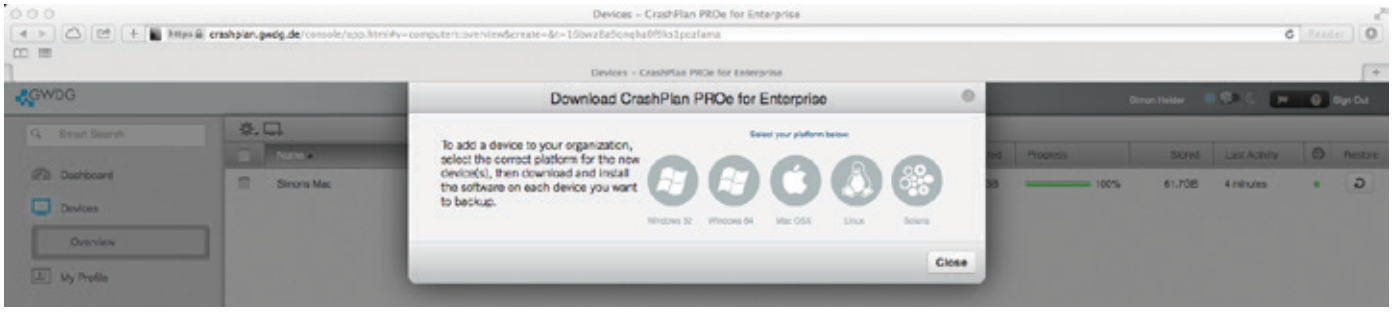


Abb. 2

auch mit dem Client erfolgen. Je nachdem, wie viele Versionen einer Datei vom Nutzer eingestellt wurden, können diese dann an einem frei wählbaren Ort wiederhergestellt werden.

NUTZUNG UND EINRICHTUNG VON CRASHPLAN PROE

Um CrashPlan PROe zu nutzen, wird ein Account im LDAP der GWDG benötigt. Da die Anzahl der Lizenzen begrenzt ist (zunächst 500), muss dem Account vorerst durch die GWDG auf dem CrashPlan-Server eine Lizenz zugeordnet werden. Bei Bedarf können aber auch mehr Lizenzen zu den Rahmenvertragskonditionen erworben werden.

Anschließend kann sich der Nutzer auf *https://crashplan.gwdg.de* einloggen (Aus Sicherheitsgründen wird immer auf die verschlüsselte „https“-Verbindung umgeleitet; siehe Abb. 1).

Nach dem Login öffnet sich ein weiteres Fenster, das die vom Server angebotenen Clients zum Download anbietet (siehe Abb. 2). Im nächsten Schritt erfolgt die Konfiguration des Clients.

Authentifizieren Sie sich zunächst mit Ihrer E-Mail-Adresse und dem dazugehörigen Passwort und tragen Sie den primären sowie den sekundären „PROe“-Server ein, wie im Screenshot angezeigt (siehe Abb. 3).

Hiermit ist die Basis-Konfiguration abgeschlossen und „GWDG Crashplan PROe“ kann genutzt werden. Wir empfehlen aber noch festzulegen, welche Daten gesichert werden sollen – als Faustregel sei an dieser Stelle vorgeschlagen, grundsätzlich das Nutzerverzeichnis zu wählen (siehe Abb. 4).

Jetzt ist der Client vollständig eingerichtet und das initiale

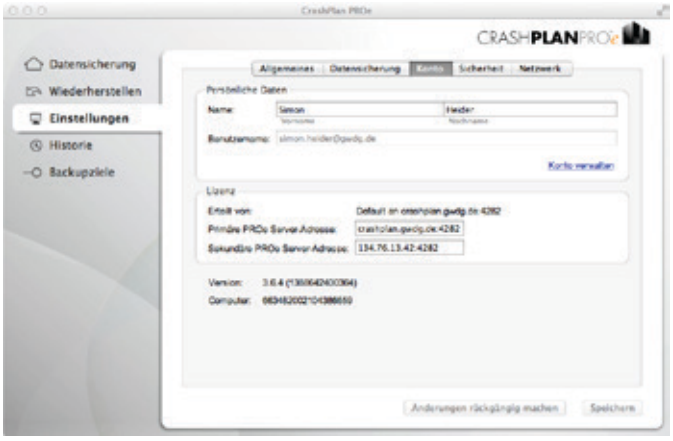


Abb. 3

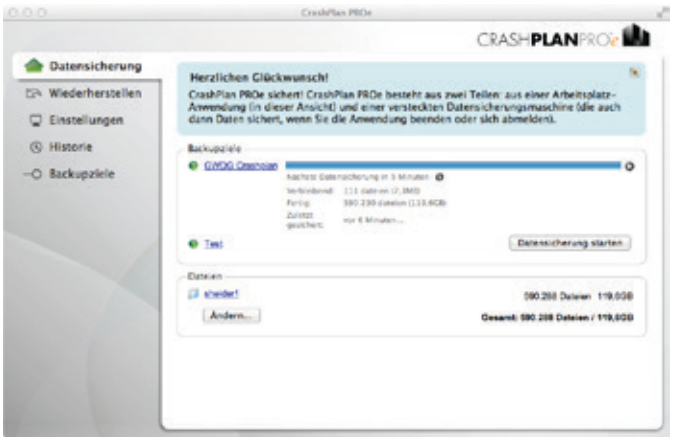


Abb. 4

Backup kann gestartet werden. Dieses dauert in der Regel recht lange, da alle Dateien erstmalig zum GWDG CrashPlan-Server übertragen werden müssen. Aus diesem Grunde empfiehlt es sich, das erste Backup aus einem schnellen Netz, z. B. über das (Kabel-)LAN aus dem GÖNET oder dem Institutsnetz (via VPN), durchzuführen. Die späteren, inkrementellen Backups können dann auch per WLAN erfolgen.

Der Client bietet darüberhinaus noch weitere Einstellungsmöglichkeiten, wie Beschränkung der genutzten Bandbreite über WLAN, aber auch stärkere Sicherheitseinstellungen wie z. B. ein zusätzliches Passwort.

Auch können zusätzlich zum PROe-Server der GWDG noch weitere Backupziele hinzugefügt werden. So kann z. B. vom Dienst-Laptop aus auch auf den Desktop-Rechner oder auf eine externe Festplatte gesichert werden. Diese Funktion empfiehlt sich vor allem, wenn große Messdateien, viele Rohdaten für Animation etc. vorhanden sind, die vorher vom Backup ausgeschlossen wurden.

Einen kleinen Wermutstropfen zum neuen Angebot können wir leider nicht verschweigen: Für die Nutzung von „GWDG CrashPlan PROe“ fallen pro Nutzer/Lizenz 26 € pro Jahr an.

Bei Interesse an der Nutzung und oder Fragen rund um „GWDG CrashPlan PROe“ wenden Sie sich bitte an *support@gwdg.de*.

FUSSNOTEN

[1] *http://www.code42.com/solutions/endpoint-backup/*
[2] *http://www.druva.com/insync/*
[3] *https://www.schneier.com/blowfish.html*
[4] *http://support.code42.com/CrashPlan/Latest/Configuring/Security_Encryption_And_Password_Options*

Kurz & knapp

Öffnungszeiten des Rechenzentrums um Ostern 2015

Das Rechenzentrum der GWDG ist vom 03.04.2015, Karfreitag, bis zum 06.04.2015, Ostermontag geschlossen.

Falls Sie sich zu der Zeit, in der das Rechenzentrum geschlossen ist, in dringenden Fällen an die GWDG wenden wollen, schicken Sie bitte eine E-Mail an *support@gwdg.de*. Das dahinter befindliche Ticket-System wird auch während dieser Zeit von Mitarbeiterinnen und Mitarbeitern der GWDG regelmäßig überprüft.

Wir bitten alle Benutzerinnen und Benutzer, sich darauf einzustellen.

Grieger

Nutzung von MS Office auch für private Zwecke

Im Zuge des abgeschlossenen Campus Agreements mit der Firma Microsoft kann nun Office 365 Professional Plus auch für private Zwecke von Studierenden sowie Mitarbeiterinnen und Mitarbeitern der Universität Göttingen genutzt werden. Die Verwendung ist sowohl lokal (lokale Installation auf dem eigenen Rechner) als auch in der Microsoft Cloud möglich. Die jährlichen Gebühren betragen 4,99 EUR. Weitere Informationen sind unter *http://www.gwdg.de/index.php?id=2997* sowie im entsprechenden Artikel in dieser Ausgabe der GWDG-Nachrichten zu finden.

Grieger

Etherpad bei der GWDG

Die GWDG stellt unter *http://etherpad.gwdg.de* einen Etherpad-Service zur Verfügung. Etherpad ermöglicht die Bearbeitung eines Dokuments durch verschiedene Nutzer in Echtzeit. Die Installation befindet sich zurzeit noch im Testbetrieb, soll aber demnächst als neuer Dienst angeboten werden. Beachten Sie bitte auch die Hinweise auf der Startseite. Nähere Informationen zur genutzten Software finden Sie unter *http://etherpad.org*.

Linnemann

Hosting von GWDG Cloud Share für externe Kunden

Die GWDG bietet auch für Kunden außerhalb der Universität Göttingen und der Max-Planck-Gesellschaft ein Hosting des bekannten und bewährten Sync&Share-Dienstes „GWDG Cloud Share“ an. Es stehen dabei zwei Modelle zur Verfügung:

1. **GWDG Cloud Share Flex** (flexible Anzahl Benutzer) und
2. **GWDG Cloud Share Flat** (Lizenzierung aller Benutzer einer Einrichtung; fast 70 % Ermäßigung gegenüber Cloud Share Flex).

Der Dienst kann auch im Rahmen der DFN-Cloud bezogen werden (siehe *https://www.dfn.de/dfn-cloud/*). Weitere Informationen finden Sie unter *http://www.gwdg.de/index.php?id=cloudshare-hosting*.

Wegmann

Neue Maßnahmen gegen Spam und Phishing-E-Mails

Text und Kontakt:
Stefan Teusch
stefan.teusch@gwdg.de
0551 201-1866

Aufgrund zunehmender Spam- und Phishing-E-Mail-Vorfälle führt die GWDG erweiterte Senderestriktionen für authentifizierte Benutzer des UNIX-Mailers *mailer.gwdg.de* bzw. *mailer.mpg.de*. ein. Zudem werden von extern eingehende Lesebestätigungen für Exchange-Benutzer unterbunden.

Bei der Filterung virenbehafteter E-Mails und auch von „unsolicited commercial e-mail" (UCE, umgangssprachlich als Spam bezeichnet) nutzt die GWDG die entsprechenden DFN-Dienste, die äußerst zuverlässig funktionieren. Sie sind jedoch machtlos, wenn unerwünschte E-Mails direkt über den zentralen UNIX-E-Mail-Server der GWDG eingeliefert werden, der noch vor dem Hauptsystem „Microsoft Exchange 2010" lokalisiert ist.

Seit Ende letzten Jahres steigt die Anzahl von UCE- und Phishing-E-Mails über diesen E-Mail-Server zunehmend an. Dies betrifft sowohl eingehende E-Mails an unsere Benutzer als auch ausgehende E-Mails, die ggfs. auch unter Ausnutzung der Absenderadressen unserer Benutzer verschickt wird. Zeitgleich ist eine neue Qualität der Einlieferungen zu beobachten: Die Sender nutzen den VPN-Service, um eine verschlüsselte Verbindung ins GÖNET aufzubauen, und senden ihre unerwünschten Botschaften somit aus lokalen Netzen.

Derartige Vorfälle sind nicht nur unangenehm; sie kosten Aufwand, Zeit und produzieren unnötige Kosten. Vor allem aber gefährden sie die Stabilität des E-Mail-Dienstes, da die E-Mail-Systeme der externen Empfänger ihre Empfangsraten drosseln oder schlicht gar keine E-Mails mehr von E-Mail-Systemen der GWDG akzeptieren. Dies betrifft dann alle Benutzer des E-Mail-Dienstes.

Aufgrund dieser unerfreulichen Entwicklung werden am 13. April 2015 eigene Maßnahmen zur Eindämmung solcher Vorfälle als auch von deren Auswirkungen vorgenommen:

- Im Exchange-Dienst wird die Anforderung von Lesebestätigungen von externen Kommunikationspartnern unterbunden. Entsprechende Bestätigungen werden nur noch innerhalb der Exchange-Umgebung möglich sein.

Die beiden folgenden Änderungen betreffen die Exchange-Nutzung nicht:

- Auf dem zentralen UNIX-E-Mail-Server *mailer.gwdg.de* bzw. *mailer.mpg.de* werden für authentifizierte Benutzer Sendelimits von 500 E-Mails pro Tag und für VPN-Benutzer von 100 E-Mails pro Tag eingeführt. Derartige Limits existieren für nicht-authentifizierte Verbindungen bereits seit Langem. Analog dazu werden nach vorheriger Anmeldung über *support@gwdg.de* auch Ausnahmen mittels Freischaltung möglich sein. Bereits bestehende Freischaltungen bleiben natürlich erhalten.
- Der sog. Mailsubmission-Dienst (TCP-Port 587), über den E-Mail-Klientenprogramme zu sendende E-Mails an den weitervermittelnden E-Mail-Server übergeben, erfordert zukünftig ausschließlich eine authentifizierte Verbindung. Auch hierfür wird eine Freischaltung nach entsprechender Anmeldung an *support@gwdg.de* möglich sein.

Beachten Sie bitte, dass der zentrale UNIX-E-Mail-Server nur in Ausnahmefällen für das Versenden von E-Mails vorgesehen ist. Regulär erfolgt der E-Mail-Versand ebenfalls über Exchange. Sofern Sie Ihre E-Mail-Klienten nicht explizit neu konfiguriert haben, sind Sie von obigen Änderungen nicht betroffen.

New actions against spam and phishing e-mails

Due to increasing amount of spam and phishing e-mail incidents GWDG enforces sending restrictions for authenticated users of the UNIX mail systems *mailer.gwdg.de* and *mailer.mpg.de*. In addition, external read receipts for Exchange users will be filtered.

Microsoft-Software für die Max-Planck-Gesellschaft und die Universität Göttingen

Text und Kontakt:
Dr. Wilfried Grieger
wilfried.grieger@gwdg.de
0551 201-1512

Für die Institute der Max-Planck-Gesellschaft standen bisher Volumenlizenzprogramme der Firma Microsoft zur Verfügung, aus denen die Software kostengünstig beschafft und genutzt werden konnte. Diese Verträge sind von Microsoft im letzten Jahr nicht mehr verlängert bzw. gekündigt worden. Die Institute der Georg-August-Universität Göttingen können auch weiterhin Software und die zugehörigen Lizenzen aus Volumenlizenzprogrammen erwerben.

MICROSOFT-SOFTWARE FÜR DIE MAX-PLANCK-GESELLSCHAFT

Campus Agreements

Die bereits vor vielen Jahren abgeschlossenen Campus Agreements wurden von Microsoft nicht mehr verlängert. Da die Software-Lizenzen aus diesen Verträgen lediglich gemietet sind, dürfen sie nicht mehr verwendet werden.

Select Plus

Der ebenfalls bereits seit vielen Jahren bestehende Select-Plus-Vertrag ist zum Ende des Jahres 2014 von Microsoft gekündigt worden. Bis dahin konnten noch Lizenzen zu akademischen Konditionen erworben werden. Da die aus diesem Vertrag beschafften Lizenzen gekauft sind, gelten sie unbegrenzt weiter. Die Software-Assurance für diese Lizenzen läuft bis zum 31.12.2017. Die Institute wurden darüber von der Generalverwaltung ausführlich informiert. Über den Select-Plus-Vertrag können nun keine neuen Software-Lizenzen mehr erworben werden.

MICROSOFT-SOFTWARE FÜR DIE UNIVERSITÄT GÖTTINGEN

Die Institute der Georg-August-Universität Göttingen haben die Möglichkeit, Microsoft-Software und die zugehörigen Lizenzen aus zwei Volumenlizenzprogrammen zu beschaffen, nämlich aus dem neuen Campus Agreement und aus dem schon seit vielen Jahren bestehenden Select-Plus-Programm. Vertragshändler ist in beiden Fällen die asknet AG in Karlsruhe.

Campus Agreement

Das Campus Agreement mit der Firma Microsoft hat die Universität Göttingen, einschließlich der Universitätsmedizin Göttingen (UMG), für den Zeitraum vom 01.10.2014 bis zum 30.04.2017 abgeschlossen. In dieser Zeit stehen den Instituten die folgenden Software-Produkte ohne Zusatzkosten in beliebiger Anzahl zur Verfügung:

- Windows Upgrade (in allen Ausprägungen)
- Windows Server
- Office Professional Plus

Microsoft software for the MPG and the University of Göttingen

For the institutes of the Max-Planck-Gesellschaft there were Volume Licensing programs from Microsoft available from which the software could be inexpensively purchased and used. These contracts were not renewed resp. were terminated by Microsoft last year. The institutes of the University of Göttingen can continue to acquire software and associated licenses out of Volume Licensing programs.

Zusätzlich sind damit alle Client Access Lizenzen (CALs), die für die Zugriffe auf die Systeme Windows Server, Exchange Server, SharePoint Server und Lync Server benötigt werden, in der Standard-Form abgedeckt.

Die jährlichen Kosten zur Finanzierung des Campus Agreements richten sich ausschließlich nach der Zahl der Mitarbeiterinnen und Mitarbeiter sowie der Studierenden und nicht nach der Zahl der eingesetzten Software-Produkte. Die Gesamtkosten werden von der Universität auf die Fakultäten aufgeteilt. Die Software ist in dem angegebenen Zeitraum lediglich gemietet.

Weitere Informationen zum Campus Agreement finden Sie auf den WWW-Seiten der GWDG unter *http://www.gwdg.de/index.php?id=2997* sowie im Mitarbeiterportal der Universität unter dem URL *https://intern.uni-goettingen.de/infocenter/it/it-service/campusvertrag*.

Beschaffung der Software

Um die Lizenzen für den Windows Upgrade aus dem Campus Agreement nutzen zu können, muss für jedes System eine Basislizenz des Desktop-Betriebssystems Windows vorliegen. Am kostengünstigsten können diese Basislizenzen zusammen mit dem Kauf der Hardware beschafft werden. Hier ist zurzeit der Dell-Rahmenvertrag zu nutzen (Dell-Shop: EBP oder eQuotes an Zentralen Einkauf). Um nachzuweisen, dass eine Basislizenz vorhanden ist, muss dieses dokumentiert werden. Bei der Bestellung über die Firma Dell ist die Dokumentation durch die Beschaffungs- und Abrechnungsdokumente gewährleistet. Bei Beschaffungen außerhalb des Rahmenvertrages muss die Dokumentation der genutzten Basislizenz von den Einrichtungen selbst vorgenommen werden.

Die Basislizenzen der folgenden Betriebssysteme sind upgradefähig:

- MacOS
- Windows 98 (auch SE)
- Windows NT 4.0
- Windows XP (Home/Starter/Pro Blade PC/Pro N/Tablet Edition/Pro)
- Windows Vista (Starter Edition/Home Basic/Home Premium/Ultimate/Business/Enterprise)
- Windows 7 (Starter Edition/Home Basic/Home Premium/Ultimate/Pro/Enterprise)
- Windows 8 (ohne Zusatz/Pro/Enterprise)

Die GWDG hat seit Oktober 2014 ein Software-Repository für alle im Campus Agreement verfügbare Software zur Verfügung gestellt, von dem die Software installiert oder zur Installation auf den lokalen Rechner kopiert werden kann. Darüber ist dann auch das Upgrade des Desktop-Betriebssystems auf eine neuere Windows-Version möglich.

Auf das Software-Repository kann über *\\wfs-msiso.top.gwdg.de\iso$* als virtuelles Laufwerk zugegriffen werden. Als Authentifizierung dienen die Benutzerkennung und das zugehörige Passwort im Active Directory der Universität.

Alle für die Installation der Software benötigten Aktivierungsschlüssel können wie bisher vom KMS-Server *ug-kms.uni-goettingen.de* der GWDG bezogen werden. Die Anzahlen der Aktivierungen werden automatisch erfasst, sodass diese Daten für eventuell spätere Lizenzverhandlungen mit der Firma Microsoft verwendet werden können. Die Nutzung des KMS-Servers wird daher empfohlen.

Eine Beschreibung zur Nutzung des KMS-Servers ist unter dem folgenden URL verfügbar: *http://www.gwdg.de/index.php?id=2953*.

Falls in begründeten Fällen der KMS-Server nicht genutzt werden kann, können die dann zu verwendenden MAK-Schlüssel von den zuständigen Helpdesks per E-Mail angefordert werden: Für die Universitätsverwaltung ist das *it@zvw.uni-goettingen.de*, für die Fakultäten ist das *support@gwdg.de*. Als Absenderadresse muss dabei die von der Universität bzw. von der GWDG vergebene verwendet werden.

Software für Studierende

Studierende können im Rahmen des Campus Agreements Office 365 Professional Plus über das von der Firma asknet bereitgestellte Portal beziehen: *https://www.studyhouse.de/cgi-bin/product/P10016549*.

Die Nutzung ist sowohl lokal (lokale Installation der Software) als auch in der Microsoft Cloud möglich. Der Nachweis der Zugehörigkeit zur Universität Göttingen erfolgt über die E-Mail-Adresse und das zugehörige E-Mail-Passwort (Shibboleth-Authentifizierung). Bei der Anmeldung ist daher die „Einrichtung" auszuwählen: Georg-August-Universität Göttingen.

Die Kosten pro Lizenz betragen pro Jahr 4,99 € (einschließlich Mehrwertsteuer). Nach Beendigung des Studiums darf die Lizenz nicht mehr genutzt werden. Die Rechnungsstellung und -abwicklung übernimmt die Firma asknet.

Software für Mitarbeiterinnen und Mitarbeiter (Work at Home, Home use)

Mitarbeiterinnen und Mitarbeiter können im Rahmen des Campus Agreements Office 365 Professional Plus über das von der Firma asknet bereitgestellte Portal beziehen: *https://www.academic-center.de/cgi-bin/product/P10016549*.

Die Nutzung ist sowohl lokal (lokale Installation der Software) als auch in der Microsoft Cloud möglich und kann sowohl für dienstliche als auch für private Zwecke (Work at Home und Home use) auf privaten Rechnern erfolgen. Der Nachweis der Zugehörigkeit zur Universität Göttingen erfolgt über die E-Mail-Adresse und das zugehörige E-Mail-Passwort (Shibboleth-Authentifizierung). Bei der Anmeldung ist daher die „Einrichtung" auszuwählen: Georg-August-Universität Göttingen.

Die Nutzung dieses Portals ist für UMG-Mitarbeiterinnen und -Mitarbeiter mit E-Mail-Adressen der Form *@med.uni-goettingen.de* zurzeit noch nicht möglich!

Die Kosten pro Lizenz betragen pro Jahr 4,99 € (einschließlich Mehrwertsteuer). Nach dem Ausscheiden aus dem Dienst der Universität darf die Lizenz nicht mehr genutzt werden. Die Rechnungsstellung und -abwicklung übernimmt die Firma asknet.

Select Plus

Das Select-Plus-Programm für die Universität Göttingen bleibt weiter uneingeschränkt bestehen. Software und Software-Lizenzen, die nicht aus dem Campus Agreement entnommen werden können, müssen weiterhin aus diesem Programm als kostengünstigste Möglichkeit beschafft werden. Dazu steht seit vielen Jahren das von der asknet AG betriebene und viel genutzte „Software-Portal Niedersachsen für Forschung und Lehre" *https://gwdg.asknet.de* zur Verfügung.

Helium Backup für Android

Text und Kontakt:
Eric Helmvoigt
eric.helmvoigt@gwdg.de
0551 201-1845

Leider ist bei Smartphones eine umfangreiche Datensicherung noch immer keine Selbstverständlichkeit, weder bei den Smartphone-Herstellern noch im Bewusstsein der Anwender. In diesem Artikel wird gezeigt, wie Sie auf einem Smartphone mit Android OS ein umfangreiches Backup von Apps und Daten erstellen können, ohne dass das gerootet sein muss.

SYNCHRONISATION UND BACKUP VON APPS UND DATEN OHNE ROOT

Bei Smartphones mit Android-Betriebssystem ist es leider noch immer keine Selbstverständlichkeit, dass sich Apps und die dazugehörigen Einstellungen sichern lassen. Derzeit werden mehrere Apps angeboten, mit denen sich dieses Aufgabe recht gut erledigen lässt, doch muss das Smartphone dazu gerootet [1] sein.

Einige Smartphone-Hersteller und auch Google bieten zwar Dienste an, um eine Synchronisation und das Backup von Einstellungen in deren Cloud zu machen, doch funktioniert das nicht bei allen Apps und auch nicht immer zuverlässig. In Android selber gibt es unter „Einstellungen" die Option „Sichern und Zurücksetzen", doch speichert diese leider keine App-Einstellungen oder -Daten, so wie es angegeben ist. Falls das Smartphone also defekt ist oder auf Werkseinstellungen zurückgesetzt werden muss, sind Ihre Daten verloren.

Vor dem oben genannten Hintergrund und dem, dass Anwender ihr Smartphone aus Garantie- oder Sicherheitsgründen nicht rooten wollen, wurden verschiedene Backuplösungen betrachtet. Dabei ist der Autor zu dem Schluss gekommen, dass eigentlich nur **Helium Backup** bleibt. Es ist zunächst einmal nicht ganz einfach in der Handhabung, doch es lohnt sich, sich damit einen Augenblick näher zu beschäftigen.

Helium Backup besteht aus einer App für Android, die im Google Play Store [2] zu erhalten ist, und einem Desktop-Client für Windows, Mac und Linux, der in der jeweils aktuellen Version direkt vom Hersteller [3] bezogen werden kann. Der Desktop-Client bietet bei dieser Lösung den enormen Vorteil, dass Apps und Daten auf den PC gesichert werden. Die Beschreibung hier erfolgt anhand des Windows-Clients.

Nach der Installation des Desktop-Clients auf dem PC sowie der App auf dem Smartphone muss Helium aktiviert werden. Dazu muss das Smartphone mit dem PC per USB-Kabel verbunden und der Desktop-Client sowie die App müssen gestartet werden.

Sind der Client und die App erfolgreich verbunden, so wird dieses mit einem grünen Häkchen im Client gemeldet (siehe Abb. 1).

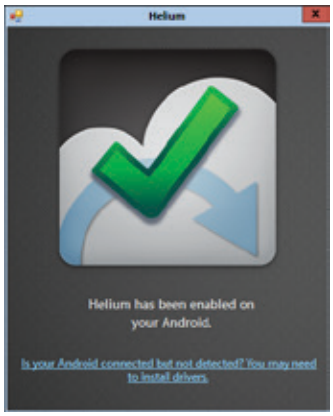


Abb. 1

Dieser Vorgang ist jedoch normalerweise nur einmal nötig, es sei denn, dass das Smartphone neu gestartet wurde.

Wird die Helium-App das erste Mal gestartet, so werden Sie aufgefordert, das USB-Debugging [4] einzuschalten, falls dieses auf Ihrem Gerät nicht bereits geschehen ist. Folgen Sie einfach den App-Anweisungen. Ansonsten gibt es erst einmal verschiedene Meldungsfenster, die von der jeweiligen Android-Version und vom Smartphone-Hersteller her unterschiedlich sind. Darunter können folgende Fenster sein (siehe Abb. 2 - 7).

Die meisten der Fenster sind selbsterklärend. Die Aufforderung aus Abbildung 4 - 6 erscheint nur bei einigen Smartphones. Das Umschalten des Verbindungstyps MTP (Media Transfer Protocol) auf PTP (Picture Transfer Protocol) ist erforderlich. Wollen Sie nach der Sicherung den Verbindungstyp wieder ändern, so wischen Sie vom oberen Displayrand nach unten. Dadurch erhalten Sie ein Fenster, in dem die Auswahl wie Abb. 6 zu sehen ist.

Setzen Sie hier das Häkchen bei Kamera (PTP). Sie erhalten danach ein Meldungsfenster mit einer entsprechenden Bestätigung (siehe Abb. 8).

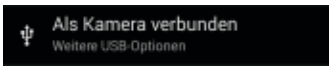


Abb. 8

Um das Backup vom PC aus durchführen zu können, muss die Helium-App auf den Smartphone gestartet sein. Tippen Sie auf die Menütaste des Smartphones unten links und wählen im sich öffnenden Menü den Auswahlpunkt „PC-Download" aus (siehe Abb. 9). Nun wird innerhalb der Helium-App der Helium-Server gestartet (siehe Abb. 10).

Der Download des Backups geschieht über das WLAN, was wiederum bedeutet, dass sich der PC und das Smartphone im gleichen Netzwerks befinden müssen. Dieses ist in Ihrem Heimnetzwerk normalerweise der Fall. Es geht auch innerhalb des eduroam-Netzwerk, wie hier im Beispiel an der IP-Adresse zu sehen (siehe Abb. 10). Wollen Sie den Server wieder ausschalten, so tippen Sie auf den großen grünen Button (siehe Abb. 10). Der Helium-Server ist ausgeschaltet wenn das rote Symbol gezeigt wird (siehe Abb. 11).

Ist Ihr Helium-Server gestartet, so wechseln Sie zum PC,

Helium Backup for Android

Unfortunately, a comprehensive backup on smartphones is still no matter of course, neither for the smartphone manufacturers nor in the consciousness of the users. This article shows how you can create a comprehensive backup of apps and data on a smartphone with Android OS without the need to be rooted.

Abb. 2

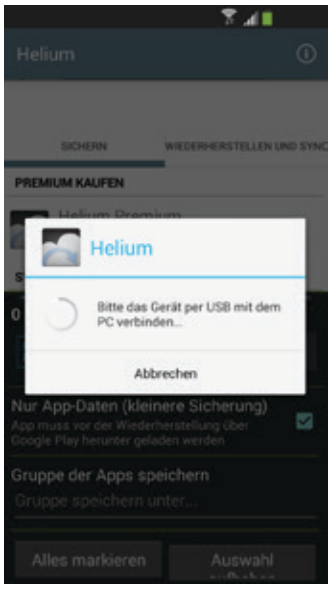


Abb. 3

Abb. 9

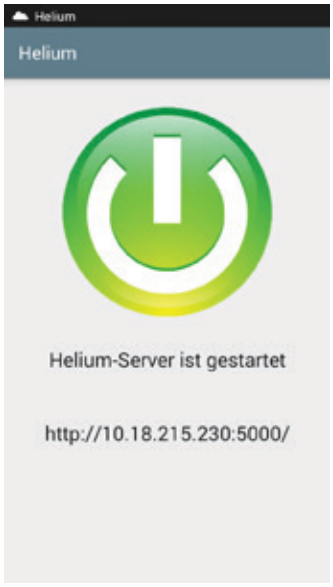


Abb. 10

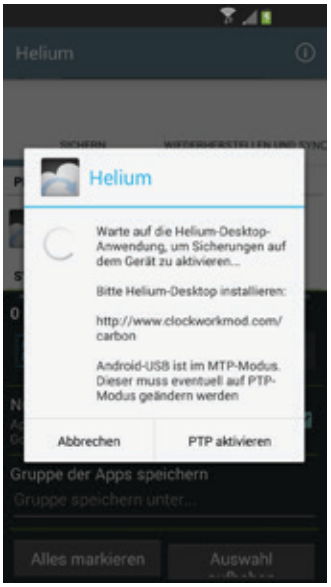


Abb. 4

Abb. 5

Abb. 6

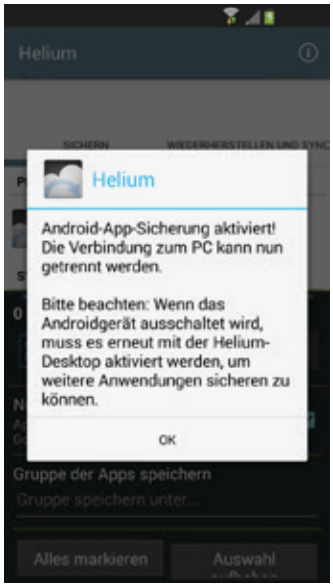


Abb. 7

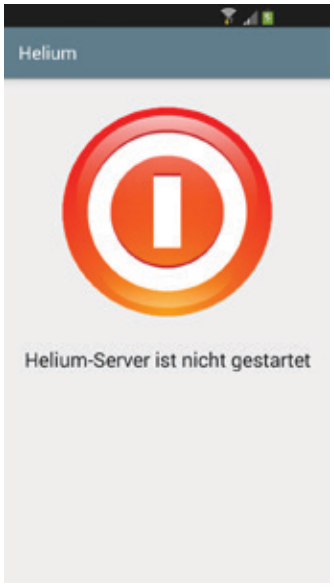


Abb. 11

starten dort einen Browser und geben als Adresse diejenige ein, welche auf dem Helium-Server angezeigt wird, in diesem Beispiel *http://10.18.215.230:5000/*. Es sollte nun eine Webseite erscheinen, auf der Ihre Smartphone-Apps aufgelistet sind, der Nachrichtenspeicher, das persönliche Wörterbuch und eine Auswahl für den Launcher [5] (siehe Abb. 12). Bei den meisten Samsung-Geräten heißt der Launcher „TouchWiz-Start".

Für ein komplettes Backup können durch das Anklicken der Schaltfläche „Select All" alle Apps ausgewählt werden. Wollen Sie nur einzelne Apps sichern, so sind diese einzeln anzuklicken. Über die Schaltfläche „Start Backup" wird die Sicherung gestartet, die Apps inkl. Ihrer Daten werden in eine ZIP-Datei namens *backup.zip* auf den PC gespeichert. Bitte achten Sie darauf, dass das Smartphone nicht im Sperrbildschirm ist, da das Backup sonst nicht funktioniert. Das Gleiche gilt beim Restore.

Für ein Restore (siehe Abb. 13) klicken Sie unter „Drop backup file here" auf die Schaltfläche „Browse" und wählen über das sich öffnende Auswahlfenster die Datei *backup.zip* aus.

Die gespeicherten Apps und Daten werden aufgelistet und ein Restore kann über die Schaltfläche „Browse" gestartet werden. Eine Auswahl einzelner Apps oder Dateien ist leider nicht möglich.

Wollen Sie einzelne aus den Restore herausnehmen, so müssen Sie innerhalb der Datei *backup.zip* die Datei *backup.json* manipulieren. Hierbei sollten Sie sich aber sicher sein was zu tun ist. In dem hiesigen Beispiel sieht der Inhalt der Datei *backup.json* wie folgt aus:

{„packages“:[{„enabled“:true,“system“:true,“flags“:8961541,“packageName“:“com.android.providers.telephony“,“versionCode“:18,“label“:“Nachrichtenspeicher“,“versionName“:“4.3-I9300XXUGNG3“,“locked“:false,“date“:1422280222079,“apk“:false,“backup“:true},{„enabled“:true,“system“:true,“flags“:10010181,“packageName“:“com.sec.android.app.launcher“,“versionCode“:17,“label“:“TouchWiz-Start“,“versionName“:“4.3-I9300XXUGNG3“,“locked“:false,“date“:1422280222163,“apk“:false,“backup“:true}]}

Wollen Sie den Launcher aus dem Restore herausnehmen, so müssen Sie den im Folgenden rot markierten Text entfernen:

{„packages“:[{„enabled“:true,“system“:true,“flags“:8961541,“packageName“:“com.android.providers.telephony“,“versionCode“:18,“label“:“Nachrichtenspeicher“,“versionName“:“4.3-I9300XXUGNG3“,“locked“:false,“date“:1422280222079,“apk“:false,“backup“:true},{„enabled“:true,“system“:true,“flags“:10010181,“packageName“:“com.sec.android.app.launcher“,“versionCode“:17,“label“:“TouchWiz-Start“,“versionName“:“4.3-I9300XXUGNG3“,“locked“:false,“date“:1422280222163,“apk“:false,“backup“:true}]}

Die einzelnen Abschnitte für eine App enden immer mit *,“backup“:true}* und sind so unterscheidbar.

Bevor Sie jedoch die Datei *backup.json* verändern, sollten Sie sich eine Kopie der *backup.zip*-Datei machen.

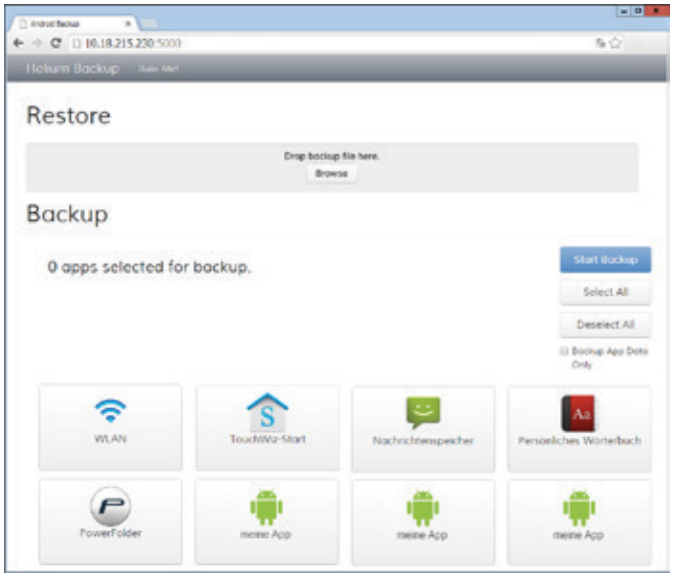


Abb. 12

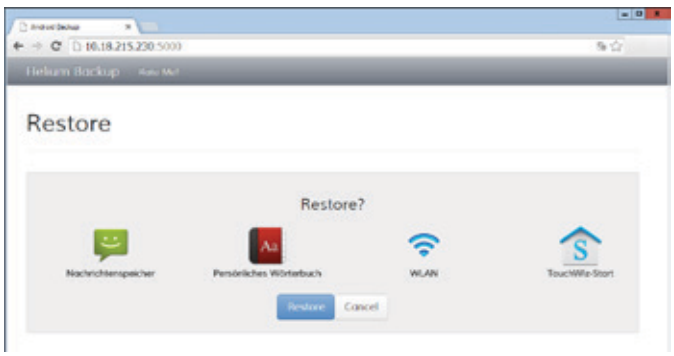


Abb. 13

EINE WEITERE MÖGLICHKEIT FÜR EIN BACKUP MIT HELIUM

Mit Helium Backup haben Sie noch weitere Möglichkeiten, ein Backup zu erstellen, z. B. auf den internen Speicher des Smartphones oder eine Speicherkarte. Weitere Optionen, wie ein Sicherungszeitplan oder die Speicherung bei den verschiedenen Cloud-Diensten sind mit der Kaufversion der App möglich. Hier wird jedoch nur noch auf das Speichern auf einer Speicherkarte eingegangen, was für die meisten Anwender ausreichend sein dürfte.

Wenn Sie Helium gestartet haben, erhalten Sie ein Startfenster, auf dem Ihnen Werbung und der Kauf der Vollversion angeboten werden. In der unteren Hälfte des Fensters steht die Liste der installierten Apps und Daten. Ganz unten befindet sich der Bereich, über den sich die Sicherung steuern lässt (siehe Abb. 14).

Im mittleren Bereich können Sie die zu sichernden Apps auswählen, durch Nachobenwischen werden weitere Apps sichtbar. Die ausgewählten Apps werden im untersten Abschnitt aufgelistet (siehe Abb. 15). Wollen Sie nicht nur die Daten der Apps sichern, sondern auch die Apps selber, so müssen Sie den untersten

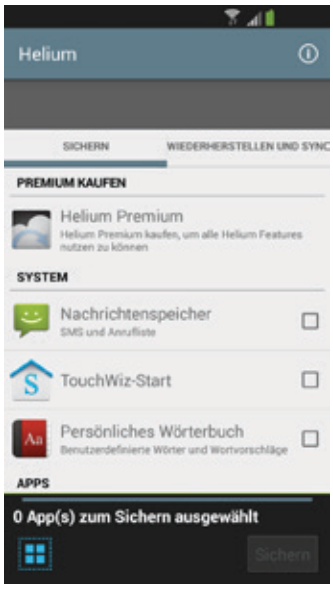


Abb. 14

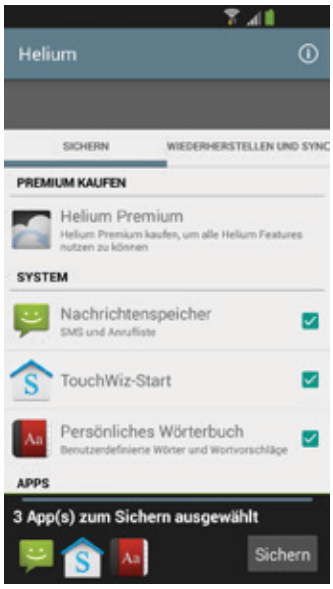


Abb. 15

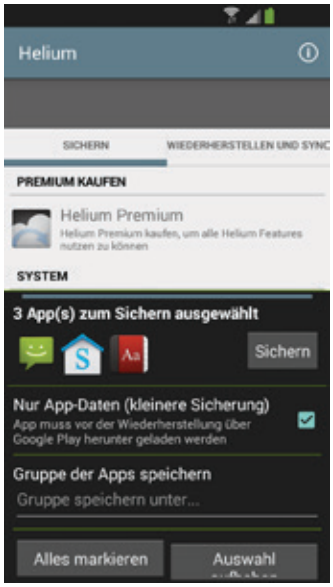


Abb. 16

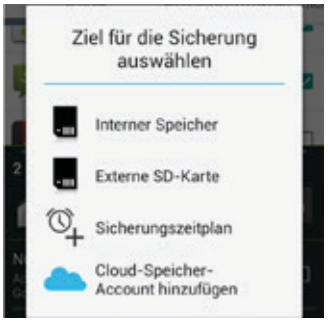


Abb. 17

Abb. 18

Abb. 19

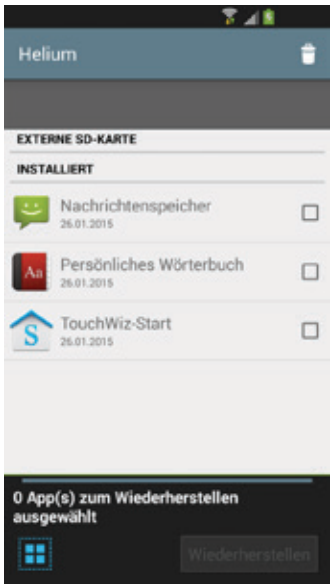


Abb. 20

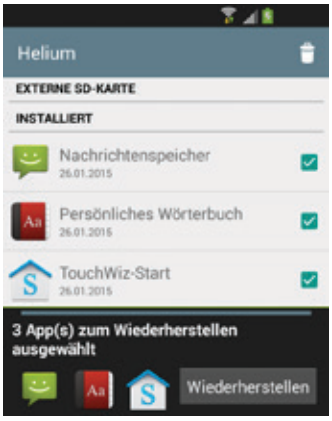


Abb. 21

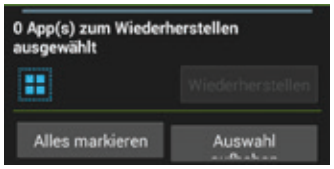


Abb. 22

Bereich durch Wischen nach oben erweitern und das Häkchen bei „Nur App-Daten (kleinere Sicherung)“ entfernen (siehe Abb. 16).

Tippen Sie nun auf die Schaltfläche „Sichern“ und wählen im nächsten Fenster den Speicherort aus (siehe Abb. 17):

Nach der Auswahl des Speicherorts, z. B. „Externe Speicherkarte“, wird die Sicherung gestartet. Die Anzeige wechselt mehrfach, was Sie so lange ignorieren können bis die Meldung erscheint, dass die Sicherung abgeschlossen ist (siehe Abb. 18).

Für einen Restore tippen Sie im Startbildschirm von Helium auf die Schaltfläche „WIEDERHERSTELLEN UND SYNC“ (siehe Abb. 14).

Als Nächstes erhalten Sie die Auswahl für den Speicherort Ihrer Sicherung. Nach der Auswahl des entsprechenden Speichers werden Ihnen die gesicherten Apps angezeigt (siehe Abb. 20), die Sie einzeln auswählen können (siehe Abb. 21). Durch Hochziehen des untersten Abschnitts erhalten Sie eine Schaltfläche „Alles markieren“ (siehe Abb. 22).

Einige wenige Apps lassen sich mit Helium-Backup nicht sichern. Das liegt daran, dass deren Hersteller kein Backup über Fremdprogramme erlauben. Solche Apps kann man dann nur mit Titanium-Backup sichern, wozu das Smartphone jedoch gerootet sein muss.

FUSSNOTEN

[1] Das Rooten eines Android-Smartphones verschafft dem Nutzer die vollen Zugriffsrechte auf das Betriebssystem.

[2] GooglePlayStore: *https://play.google.com/store/apps/details?id=com.koushikdutta.backup*

[3] Hersteller: *http://www.clockworkmod.com/carbon*

[4] USB-Debugging: Durch diese Option ist es Entwicklern oder Programmen möglich, bestimmte Aktionen auf dem Smartphone vom PC aus zu steuern.

[5] Der Launcher ist vergleichbar mit dem Desktop eines Windows-Rechners. Dort liegen z. B. Verknüpfungen der Apps, das Hintergrundbild usw.

Nutzung von Web-Diensten in der DFN- und eduGain-AAI

Seit 2014 betreibt die GWDG für ihre Kunden mehrere Identitätsprovider (IdP), die den Zugang zu föderierten Web-Diensten in der DFN- und eduGain-AAI ermöglichen. Zum einen können Mitarbeiter von Max-Planck-Instituten, die über das MetaDir der GWDG angeschlossen sind, über einen Shibboleth-IdP authentifiziert werden. Zum anderen werden Studierende und Mitarbeiter der Georg-August-Universität Göttingen ebenfalls über einen weiteren Server identifiziert. Wir sorgen dabei für den größtmöglichen Schutz von privaten Daten. Unter anderem findet die Authentifizierung an unseren Servern statt und die Kunden entscheiden in letzter Instanz, welche Attribute nach der Authentifizierung an den jeweiligen Web-Dienst weitergegeben werden (dies muss nur einmal pro Dienst durchgeführt werden).

Aktuell wollen wir hier eine kleine Auswahl an Web-Diensten präsentieren, die Ihnen über die DFN- bzw. eduGain-AAI und Shibboleth zur Verfügung stehen:

- **DFNVC Webkonferenzen** (Anmeldung für Veranstalter): *https://webconf.vc.dfn.de*
- **SiROP** (Research-Suchmaschine): *https://www.siropglobal.org*
- **GIGAMOVE** (Transfer von großen Dateien): *https://gigamove.rz.rwth-aachen.de*
- **Foodle** (Kollaborative Terminfindung): *https://foodl.org*

Neben diesen Diensten können u. a. Studierende und Mitarbeiter der Universität Göttingen auch Produkte wie z. B Microsoft Office 365 Professional Plus zu vergünstigten Konditionen von der Firma asknet über die Shibboleth-Authentifizierung beziehen (siehe auch den entsprechenden Artikel in dieser Ausgabe der GWDG-Nachrichten):

- Studierende der Universität Göttingen: *https://studyhouse.de*
- Mitarbeiter der Universität Göttingen und der GWDG: *https://www.academic-center.de/cgi-bin/product/P10016549*

Adler

Die Rückkehr des GDB-Ritters

Text und Kontakt:
Thorsten Hindermann
thorsten.hindermann@gwdg.de
0551 201-1837

Mit der Umstellung von Apple auf die neue Compiler-Infrastruktur LLVM (*http://llvm.org*) wurde der GNU C-Compiler nebst Fehlersuchprogramm (engl. Debugger) GNU Debugger, kurz gdb, vom Entwicklungsprogramm Xcode entfernt. Viele andere Entwicklungsprogramme setzen aber noch auf eine Integration des gdb und haben noch nicht auf die neue Schnittstelle zum Fehlersuchprogramm lldb der LLVM Compiler-Infrastruktur umgestellt. In diesem Artikel soll am Beispiel der Lazarus-Entwicklungsumgebung (Delphi-Klone) gezeigt werden, wie der gdb wieder zum Einsatz kommen kann.

ANGRIFF DER KLONE-IDE

Der Autor dieses Artikels hat in seiner frühen Phase der Anwendungsentwicklung lange Jahre Pascal-Programme mit Borland Turbo Pascal (3.0 – 7.0) für MS-DOS und später mit Borland Delphi für Windows entwickelt. Als Hobby in seiner Freizeit bleibt er dieser Programmiersprache noch immer „treu“ und programmiert unter anderem noch Pascal-Programme mit Hilfe des Free Pascal-Compiler (*http://freepascal.org*) und des Delphi-Klone Lazarus (*http://www.lazarus.freepascal.org*). Lazarus ist ein sehr gut gelungener Delphi-Klone, und mit dieser integrierten Entwicklungsumgebung (engl. Integrated Development Environmet, kurz IDE) können heute wie damals Programme schnell entwickelt werden, und zwar nach dem RAD-Prinzip (Rapid Application Development). Um nun Programmierfehler in den mit dieser IDE programmierten Pascal-Programmen zu suchen, zu finden und zu beheben, wird der Debugger **gdb** benötigt. Leider hat Apple auf seinen aktuelleren Entwicklungsversionen von Xcode den **gdb** entfernt und durch **lldb** ersetzt. Die IDE Lazarus setzt aber noch auf die gdb-Schnittstelle. Es nützt auch nichts, den lldb in den Debugger-Einstellungen der Lazarus-IDE einzutragen; das führt zu Fehlermeldungen beim Ausführen dieses Debuggers.

DAS GNU-IMPERIUM SCHLÄGT ZURÜCK

Für Mac OS X können fehlende Anwendungen und Hilfsprogramme per sogenannter Mac-Ports nachinstalliert werden. In diesem Umfeld tummeln sich drei Mac-Ports-Anbieter: MacPorts (*http://macports.org*), Fink und HomeBrew. Anhand von MacPorts werden hier nun die Anweisungen gezeigt. Für das entsprechende Mac OS X muss die richtige Version von MacPorts heruntergeladen und installiert werden. Nach der Installation ein Terminal öffnen und den Befehl *sudo port install gdb-apple* eingeben.

Nach einer Weile ist die Ausführung dieses Kommandos beeendet. Mit dem Befehl *which gdb-apple* kann der Erfolg der Aktion überprüft werden. Der Befehl sollte den Pfad */opt/local/bin/gdb-apple* zurückgeben.

Dieser Pfad kann in den Debugger-Einstellungen von Lazarus eingegeben werden, die über das Menü „Werkzeuge > Einstellungen“ und dann in der Navigation des nun erscheinenden Dialogs auf der linken Seite unter dem Knotenpunkt „Debugger“ einzutragen sind (siehe Abb. 1).

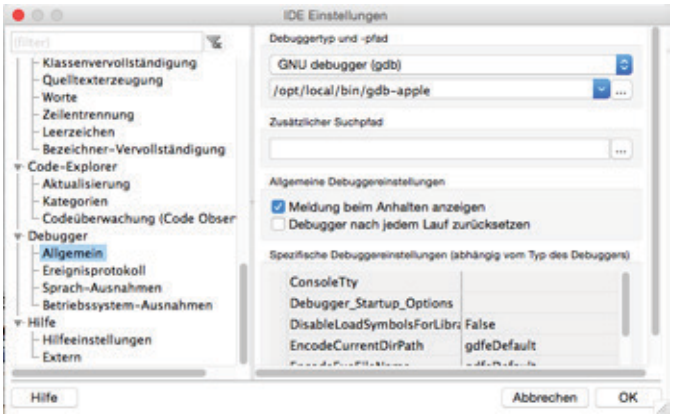


Abb. 1

Den Dialog mit „OK“ bestätigen. Beim ersten Debug-Versuch erscheint leider eine wenig ermutigende Fehlermeldung (siehe Abb. 2).

The return of the GDB knight

With Apple´s switching to the new compiler infrastructure LLVM (*http://llvm.org*), the GNU C compiler together with the GNU debugger gdb were removed from the development program Xcode. However many other development programs still bank on an integration of gdb and have not switched to the new interface for the debugger lldb of the LLVM compiler infrastructure. This article should show by the example of the Lazarus IDE (Delphi clones), how the gdb can be used again.

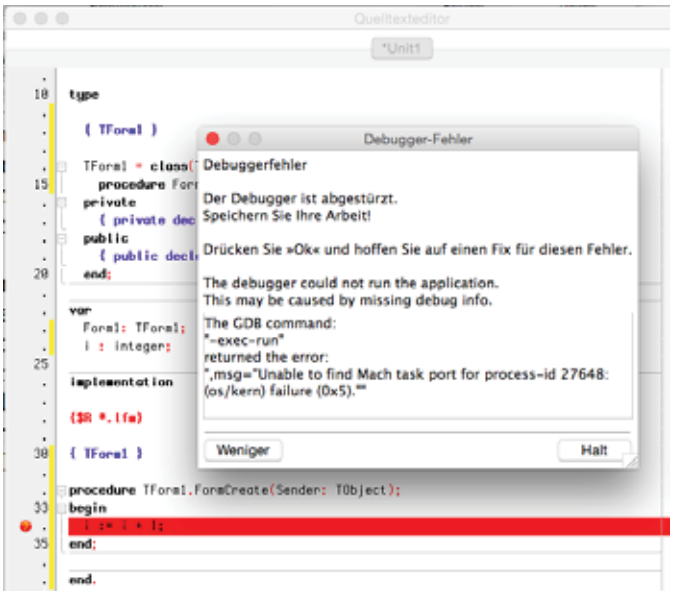


Abb. 2

DIE HOFFNUNG STIRBT ZULETZT

In der Fehlermeldung in Abb. 2 wird ja die Hoffnung geäußert, dass es eine Lösung für die Fehlermeldung gibt. Und ja, diese Lösung gibt es! Die Lösung heißt Codesigning-Zertifikate auf Basis von X.509-Zertifikaten aus der MPG-, Uni-Göttingen- oder GWDG-CA. Die Beantragung, Sicherung und der Import in die Schlüsselbundverwaltung von Mac OS X können den ersten beiden Teilen der GWDG-Nachrichten-Ausgabe Special 01/2014 entnommen werden. Bei der Beantragung ist noch wichtig, dass im Feld „Name" folgende Zeichenkette eingegeben wird (siehe Abb. 3 am Beispiel des Autors): *PN: <Vorname Nachname> (Codesigning)*

Der RA-Operator kann an diesem Pseudonym erkennen, dass er die Rolle von „User" auf „Code Signing" umstellen muss, da es sich bei diesem Zertifikat um ein Codesigning-Zertifikat handelt.

Nach dem Import des Zertifikats das importierte Zertifikat doppelt anklicken und in dem Informationen-Dialog „Vertrauen" erweitern. Unter dem Eintrag „Code-Signierung" in der Auswahlliste „Immer vertrauen" auswählen (siehe Abb. 4).

Beim Beenden dieses Dialogs muss noch das Kennwort für den administrativen Benutzer dieses Mac OS X eingeben werden, damit diese Änderung des Vertrauens gespeichert werden kann.

Für die folgenden Schritte ist es wichtig, dass die Schlüsselbundverwaltung beendet wurde.

Mit folgendem Befehl im Terminal die Prozess-Kennung von *taskgated* ermitteln: *ps aux | grep taskgated | grep -v grep*

Nun dieses Programm mittels folgendem Befehl beenden: *sudo kill -9 <Prozess-Kennung>*

Das Kennwort des administrativen Benutzers des Mac-OS-X-Systems muss eingegeben werden.

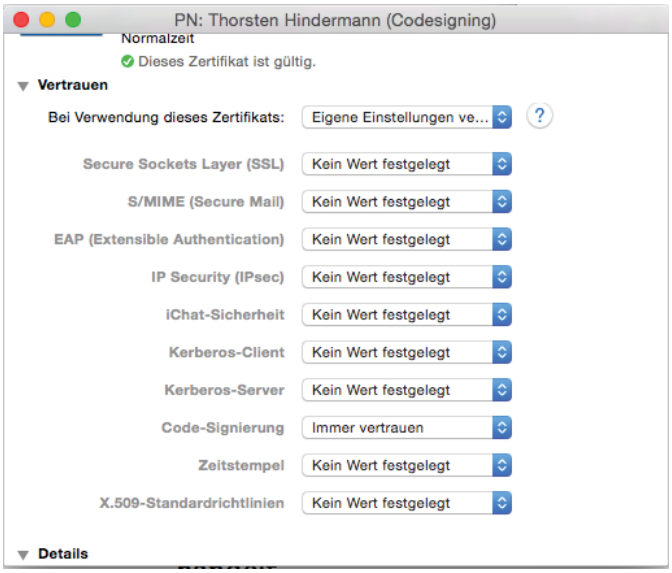


Abb. 4

Nun folgenden Befehl eingeben:

sudo codesign -s <Name des Zertifikats in der Schlüsselbundverwaltung> $(which gdb-apple)

Konkret, im Fall des Autors, muss Folgendes eingegeben werden:

sudo codesign -s PN\:\ Thorsten\ Hindermann\ \(Codesigning\) $(which gdb-apple)

Wichtig ist, dass der Doppelpunkt und die Leerzeichen mit dem Backslash *(\)* escaped werden. Folgende Dialogbox erscheint (siehe Abb. 5).

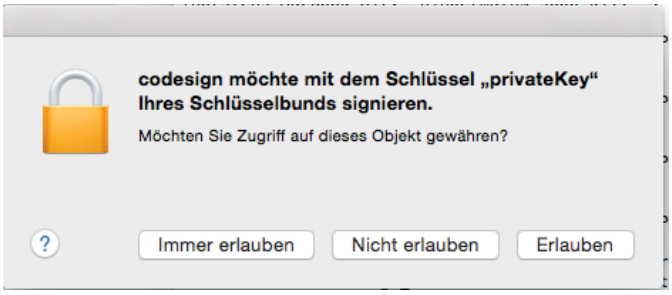


Abb. 5

Hier muss „Erlauben" oder „Immer erlauben" angeklickt werden.

DIE ZERTIFIKATSCHLACHT IST GEWONNEN UND GDB ÜBERNIMMT

Nun wieder Lazarus aufrufen, ein paar Quellzeilen eingeben und einen Haltepunkt (engl. Breakpoint) für den Debugger setzen. Das Programm wird mit *cmd+R* übersetzt und automatisch gestartet. Nun erfolgt ein Dialog mit einer Nachfrage (siehe Abb. 6).

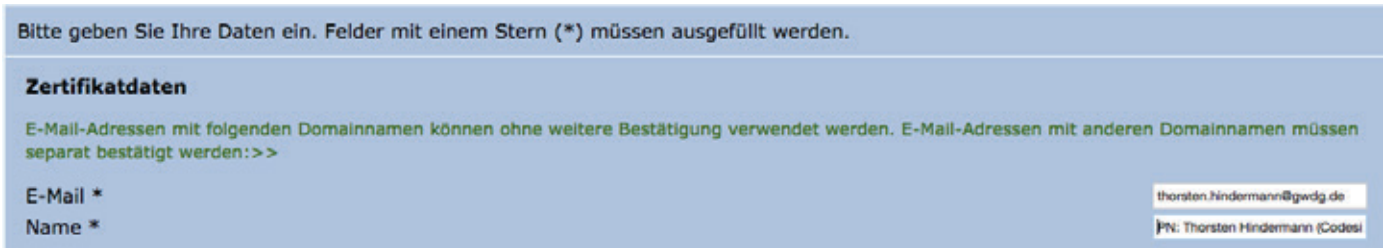


Abb. 3

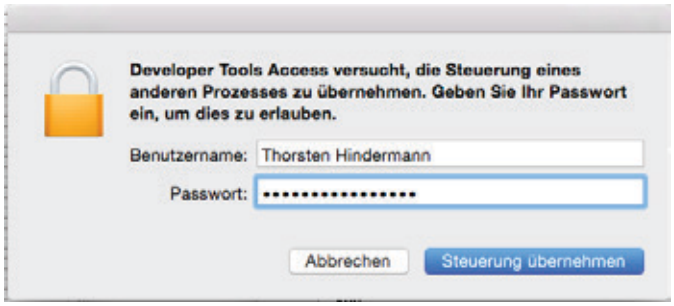


Abb. 6

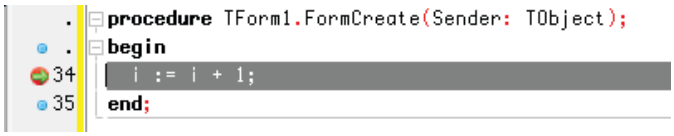


Abb. 7

Abb. 8

Hier bitte „Steuerung übernehmen“ anklicken. Wenn die Programmausführung nun am Haltepunkt unterbricht, kommt nicht mehr die Fehlermeldung vom Anfang, sondern im Bearbeitungsfenster sieht der Haltepunkt nun wie folgt aus (siehe Abb. 7).

Jetzt können die entsprechenden Debugger-Befehle abgesetzt werden (siehe Abb. 8). und das Pascal-Programm kann auf Programmier- oder Logikfehler untersucht werden. Somit kehrt der Debugger gdb wieder zurück und steht fortan Lazarus und weiteren Programmen zur Verfügung, die auf die gdb-Schnittstelle aufbauen.

Horizon 2020 Project “Mikelangelo” – Optimising Virtual Infrastructures for fast I/O

Text und Kontakt:
Peter Chronz
peter.chronz@gwdg.de
0551 201-2163

Mikelangelo belongs to the first projects funded by the European Commission as part of the Horizon 2020 research and innovation programme. This project aims to disrupt cloud computing across the whole virtual infrastructure stack. The project covers applications in cloud computing, high performance computing, and big data. GWDG belongs to the initiators of the project proposal and is now a member of the Mikelangelo’s core consortium.

SUMMARY

The European commission has granted funding to the Mikelangelo project. GWDG is a partner of Mikelangelo’s consortium. Mikelangelo belongs to the first projects funded as part of the EU’s Horizon 2020 research and innovation programme. The project aims to disrupt cloud computing across the whole virtual infrastructure stack. This stack covers virtualisation technology, operating systems, cloud middleware, big data stacks, and high performance computing (HPC). The consortium will work to improve the I/O performance of virtualised infrastructures and applications running on those infrastructures. More concretely, we will work on a new hypervisor (sKVM), a new operating system (OSv), new communication methods via remote direct memory access (RDMA), integration with OpenStack, and HPC batch systems. Thus, the project covers the whole software range of the modern computing stack for a broad set of use cases. These use cases span the applications in the fields of big data, HPC, and cloud computing. We will publish updates on the project status throughout the project duration in GWDG News. For more up-to-date news, please visit our web site (*http://www.mikelangelo-project.eu*) and follow us on Twitter (*mikelangelo_eu*) and LinkedIn (*mikelangelo_eu*). If you have a large data set, and if you are interested to become an early adaptor of novel technogies by contributing a big data use case, please contact the author.

INTRODUCTION

GWDG takes part in Mikelangelo as core member of the consortium. Mikelangelo belongs to one of the first projects funded as part of the EU's Horizon 2020 research and innovation programme. The project aims to disrupt cloud computing across the whole virtual infrastructure stack. This stack covers virtualisation technology, operating systems, cloud middleware, big data stacks, and HPC. The European Commission has granted nearly 6 million Euros to 9 partners across Europe and Israel for this 36 months long project. Figure 1 lists the partners who include four small and medium-sized enterprises (SMEs), two Universities, and two large enterprises.

Partners

PARTNER	COUNTRY
XLab	Slovenia
HLRS	Garmany
GWDG	Germany
Huawei	Germany
IBM	Israel
Pipistrel	Slovenia
Ben Gurion University	Israel
Cloudius Systems	Israel
Intel	Ireland

Figure 1_Mikelangelo Consortium

The project's consortium envisages significant improvements to the efficiency, security, and usability of cloud computing through its new developments. In practice, cloud computing relies heavily on virtualisation. Virtualisation offers near-zero overhead for computation. However, virtual machines (VM) have an efficiency of only about 60-70% for I/O operations. This overhead limits the applications that clouds can host reasonably. For example big data, HPC, and real-time applications are traditional domains in which virtualisation has found only limited application.

In this project, the consortium aims to increase I/O efficiency to nearly 100%, in an improved hypervisor, called sKVM. Furthermore, the consortium will continue development on a new operating system, called OSv, which one of the project members built specifically for cloud computing. Both sKVM and OSv will receive further extensions that will allow for efficient communication via RDMA. GWDG will then integrate both sKVM and OSv with OpenStack, to provide the advancements in a productive environment to users of infrastructure services. This integration with OpenStack will include a novel application deployment model, based on OSv. Four use cases will then leverage those advancements. GWDG's use case will offer Big Data clusters on demand. Another use case will offer cloud bursting. The remaining two use cases will offer HPC with VMs. At the end of the project GWDG aims to offer big data and HPC services on demand to its customers.

The project's scope and its merits can be best explained in a bottom-up fashion according to its architecture. Figure 2 shows Mikelangelo's architecture, which is described in the following paragraphs.

The hardware infrastructure lies at the bottom of the architecture. The hardware infrastructure includes servers, storage systems, and networking hardware. The actual hardware lies out of the scope of the Mikelangelo project.

Above the bare metal layer lies the virtualisation layer, which may include an operating system and a hypervisor. In the virtualisation layer, the project will develop an improved hypervisor, called sKVM. Here, the engineers will focus to reduce the I/O overhead and security of the virtualisation. Furthermore, the engineers will integrate RDMA with sKVM, to allow for fast and flexible communication between VMs. This layer represents the core of the Mikelangelo project, since very fast I/O in VMs is one of the project's

Key Facts

Duration: 01.01.2015 – 31.12.2017 (36 months)
Programme: H2020
Partners: 9 Partners across Europe and Israel
Funding: Grant amount 6 million EUR

Co-funded by the Horizon 2020
Framework Programme of the European Union

Horizon 2020 Projekt „Mikelangelo"

Die Europäische Kommission fördert das Projekt „Mikelangelo", welches von der GWDG mit initiiert wurde, seit dem 1. Januar 2015. Mikelangelo ist eines der ersten Projekte, welches im Zuge des Forschungs- und Innovationsprogramms Horizon 2020 der Europäischen Union gefördert wird. Das Projekt zielt darauf ab, Cloud Computing entlang der gesamten Architektur virtueller Infrastrukturen zu revolutionieren. Diese Architektur deckt Virtualisierungstechnologie, Betriebssysteme, Cloud-Middleware, Big Data Stacks und Hochleistungsrechnen ab. Das Konsortium wird daran arbeiten, die Performanz von Ein- und Ausgabeoperationen virtueller Infrastrukturen sowie den darauf aufsetzenden Anwendungen zu verbessern. Konkret wird das Konsortium an einem neuen Hypervisor (sKVM), einem neuen Betriebssystem (OSv), neuen Kommunikationswegen mittels verteiltem Speicherdirektzugriff (RDMA), einer Integration mit OpenStack und einem HPC-Batchsystem arbeiten. Folglich beschäftigt sich das Konsortium mit der gesamten Spannweite der Softwareentwicklung für moderne Rechenarchitekturen für eine große Auswahl von Anwendungsfällen. Diese Anwendungsfälle umfassen die Gebiete Big Data, Hochleistungsrechnen und Cloud Computing. Wir werden im Weiteren über den Projektverlauf in den GWDG-Nachrichten berichten. Sie können zudem den aktuellsten Entwicklungen des Projekts auf unserer Webseite (*http://www.mikelangelo-project.eu*), bei Twitter (*mikelangelo_eu*) und bei LinkedIn (*mikelangelo_eu*) folgen. Falls Sie daran interessiert sind, als „Early Adaptor" große Datenmengen im Zuge eines Big-Data-Anwendungsfalls der GWDG zu verarbeiten, melden Sie sich bitte beim Autor dieses Artikels.

main promises. The architecture leverages fast VM I/O throughout the whole stack. I/O is that important since data processing is one of the major tasks of virtual infrastructures. Moreover, data growth even outstrips the gains in networking and computing performance.

OSv represents the third layer in Mikelangelo's architecture. OSv is a new operating system built from scratch specifically for cloud computing. In this project, engineers will extend OSv to run HPC and big data applications. Furthermore, the engineers will integrate RDMA with OSv, and improve application deployment via Capstan. Capstan is OSv's deployment mechanism, which resembles Docker. OS'v major benefits are high performance, a low footprint, and full VM isolation through virtualisation.

OpenStack comes next in the architecture. OpenStack is the project's cloud middleware of choice, to leverage sKVM and OSv. The project's improved version of OpenStack will use sKVM for virtualization and OSv as preferred operating system for VMs. Moreover, GWDG will integrate Capstan in the cloud layer, to deploy a large number of applications conveniently via various user interfaces. In addition, the cloud layer will feature advanced monitoring across all layers of our architecture, even for user-deployed applications.

On top of the cloud and virtualisation layer, big data and HPC applications will serve as use cases. The big data applications target primarily Apache's big data stack including Hadoop, which will be managed using Apache Sahara. The HPC use cases will run a batch system, which will execute OpenFOAM simulations and custom simulations of cancellous bones. Both use cases aim to allow customers to use clusters on demand with customised environments. At the same time the use case will offer top computational and I/O efficiency. Currently, big data and HPC applications typically do not use cloud computing, mostly because of the low I/O performance. However, both areas can benefit greatly from the cloud paradigm, since it offers a lot of flexibility.

In this article we provide a summary about the project's goals and approach, including basic background knowledge. The article further contains information how we are going to progress beyond the state of the art. The remainder of this article presents more details on Mikelangelo's technical merits in a bottom-up fashion according to Figure 2.

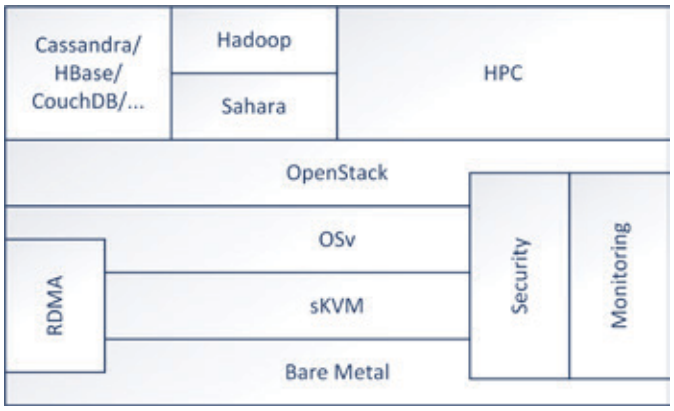


Figure 2_Mikelangelo´s architecture

A HYPERVISOR WITH OPTIMISED I/O PROCESSING: SKVM

The Mikelangelo project introduces an improved version of the kernel-based virtual machine (KVM) hypervisor. To bring KVM into the context of virtualisation technology at large, we first provide an overview of virtualisation technology. Then we describe our advancements beyond the state of the art.

Hypervisors, such as KVM, execute and manage VMs. Traditionally those hypervisors fall into two different categories. The first category contains, the so called, type 1 hypervisors. These hypervisors are also known as bare-metal hypervisors. Type 1 hypervisors run directly on the hardware without any fully fledged operating system beneath the hypervisor. Examples for these hypervisors are VMWare ESX, Xen, and Hyper-V. Type 2 hypervisors run in user-space of a base operating system. Examples for type 2 hypervisors are Linux-VServer, Linux containers and BSD jails, OpenVZ, QEMU, and KVM. Nowadays, hypervisors such as KVM blur these boundaries, since they consist of kernel modules, which run in kernel mode.

Mikelangelo will base its work on KVM. KVM is a popular hypervisor technology, which uses Linux as host system. KVM supports nearly arbitrary guest operating systems, has an open source license, and provides good performance. These features make KVM popular, especially in the context of cloud computing. Typically OpenStack-based clouds use KVM. However, KVM provides below-native performance. Although KVM offers near-zero overhead for compute virtualisation, its I/O virtualization efficiency lies around 60-70%. Here I/O refers to network communication and to disk access.

In Mikelangelo, engineers at IBM will improve KVM with regards to I/O performance. The performance improvements will come from a new I/O scheduler that will be transparent to the guest system. This I/O scheduler will allocate resources for the I/O activity of guests, thus for virtual I/O. Currently, such a virtual I/O scheduler does not exist. However, previous research by IBM on a software called Elvis promises good results with this approach.

A NEW OPERATING SYSTEM FOR THE CLOUD: OSV

OSv is the preferred guest operating system in Mikelangelo's cloud stack. OSv is an operating system developed from scratch by the start-up Cloudius Systems. Cloudius, who are part of Mikelangelo's consortium, have developed OSv specifically for cloud computing. In the following paragraphs we describe the motivation behind OSv and then Mikelangelo's improvements to OSv.

Currently, clouds mostly run guest OSs with well-known operating system such as Ubuntu, Debian, and CentOS. Most of the time these guest systems use Linux as foundation. Some more specialised systems such as CoreOS are stripped-down versions of Linux. The downside of the Linux approach to Cloud guests lies in its inefficiency. Linux has not been developed specifically to be run as a guest OS in a cloud. Thus, Linux carries a lot of unnecessary baggage in form of legacy code that was intended for other purposes. This legacy codes leads to inefficiencies. These inefficiencies, in turn, become apparent in start-up times, lowered computational throughput, and disk image size.

Containers, such as Linux containers, BSD jails, and OpenSolaris zones, offer an alternative and a more lightweight approach to virtualisation. However, containers have multiple disadvantages. One disadvantage lies in the inherent difficulty to isolate containers well from the host operating system. This lack in isolation

offers a vulnerability. Another major disadvantage of containers lies in the constraint of the operating system. A container offers controlled access to the host operating system. Thus, it is not possible to run a Windows host within a Linux container. Currently, containers are very popular as base-technology for Docker, which offers quick deployment of applications and their dependencies. Consequently, one would ideally use full virtualisation with a low footprint on resources. OSv aims to deliver exactly this small footprint, as far as the guest operating system can influence the performance.

Mikelangelo will improve OSv in three major areas: general efficiency, application support, and application packaging. To increase the general efficiency, engineers will improve the SMP load balancer in the scheduler, on one hand. On the other hand, the engineers will reduce the boot time and footprint on host system resources. Mikelangelo will improve application support, by adding additional unmodified executable formats, such as PIE, standard executables, and statically-linked executables. To provide further application compatibility, OSv will support additional functions in the Linux/Glibc ABI. Finally, Mikelangelo will improve some function implementations in OSv, such as epoll(), to support more runtime environments, such as ruby, go, and node.js. To improve application packaging and deployment, Mikelangelo will extend Capstan. Capstan is a system for application deployment, which resembles Docker. In contrast to Docker, Capstan uses OSv in a fully virtualised environment. Mikelangelo will furthermore integrate Capstan with the cloud layer to deploy applications with convenient interfaces.

FAST AND FLEXIBLE COMMUNICATION IN THE CLOUD: RDMA-BASED SHARED MEMORY

RDMA-based shared memory offers a flexible and highly performant way for VMs to communicate with each other. VMs communicate a lot with each other, since they often host different parts of distributed services and service components. VM communication becomes important, especially in the context of a one-application-per-VM model, as envisioned with OSv. In Mikelangelo, with OSv as de facto application container, inter-process communication (IPC) works via inter-VM communication. In the following paragraphs, first we describe methods for inter-VM communication and the state of the art for RDMA. Then, we describe how Mikelangelo is going to advance RDMA technology.

If two VMs reside on the same host, they can use shared memory for IPC. This type of communication between VMs promises data transfers with the highest bandwidth and lowest latency. Implementations of inter-VM IPC use either MPI or sockets as interfaces. In both cases, one can use shared memory in the backend. Some implementations are even able to switch seamlessly to a TCP/IP-based communication, when remote VMs wish to communicate. Here, we refer to remote VMs as VMs that do not reside on the same host. Communication over the TCP/IP stack allows remote communication, however the TCP/IP stack incurs an extra overhead. This overhead stems from a complex software stack in the local and remote hypervisor.

RDMA is a low-latency and high-bandwidth communication alternative to TCP/IP. RDMA works with both, Infiniband and Converged Ethernet, as physical layer. However, most RDMA implementations push RDMA semantics and interfaces into the VMs, which complicates their driver and networking subsystem. Furthermore, when VMs on the same host communicate the hypervisor needs to copy memory, unnecessarily.

Nahanni, which uses KVM, provides an alternative mechanism for inter-VM communication that differs from MPI, sockets and RDMA. Nahanni provides shared memory access between VMs without any special abstraction in the VMs. Furthermore, Nahanni uses direct shared memory pools to provide scale-out for applications such as in-memory databases. However, Nahanni focuses on intra-host communication. NetVM, builds on Nahanni to combine shared memory communication with network processing. To provide an efficient implementation NetVM maps and forwards network packets between VMs on the same host via shared memory.

Mikelangelo aims to advance the state of the art by providing netchannels for TCP/IP, improved communication APIs, RDMA integration with OSv, and para-virtualised drivers for legacy applications. Netchannels implement the socket API with TCP/IP, which works more efficiently and stable than the traditional TCP/IP stack. Mikelangelo's new communication APIs will provide more efficient I/O, zero-copy, and improved cache-efficiency. The integration of RDMA within OSv will feature a lightweight RDMA-like communication interface. To support legacy applications, Mikelangelo will develop para-virtualised I/O device drivers, which will use RDMA as a backend. These para-virtualised devices can then take advantage of zero-copy and lightweight abstraction.

IMPROVED SECURITY FOR VIRTUAL MACHINES

Clouds co-host VMs for multiple tenants. Thus Mikelangelo needs to take care of existing vulnerabilities and new ones arising in sKVM. Security poses a major concern in virtualised environments, in cloud computing, and in co-hosted, multi-user, and multi-tenant systems in general. Mikelangelo's architecture needs to ensure security in depth by respecting security issues in the host OS, hypervisor, and in the cloud middleware. The host offers an attack surface via side channel attacks. The hypervisor offers an attack surface via VM escapes and shared memory. In the following paragraphs, first, we describe the main security concerns that we need to deal with. Then, we describe how we intend to cope with those security concerns.

With a side channel attack, a malicious VM can try to access information on other tenant virtual machines, by various side channels. The most notable side channel uses timing attacks on a cache. In timing attacks malicious VMs exploit the fact that a cache is a shared resource. Shared resources, in turn, may leak information about co-located processes. State-of-the-art systems do not protect against co-tenancy side channel attacks beyond providing physical VM isolation on a physical host. VM escape exploits refer to ways for a malicious VM to escalate its privileges. An escaped

Contacts

Peter Chronz (*peter.chronz@gwdg.de*, author)
Maik Srba (*maik.srba@gwdg.de*)
Christopher Menke (*christopher.menke@gwdg.de*)

WWW: *http://www.mikelangelo-project.eu*
Twitter: mikelangelo_eu
LinkedIn: mikelangelo_eu

VM executes with the same permissions as the hypervisor itself. Thus an escaped VM can read or modify the data of other VMs, which run on the same physical host. Such VM escapes do occur in practice, which leads to exploits, such as Cloudburst in VMware and Virtunoid in KVM. A hypervisor that allows shared memory between VMs, either remotely by RDMA or locally by ivshmem, may provide additional attack vectors. Such attacks may include eavesdropping, traffic modification or buffer overflow attacks over a remote connection and uncontrolled DMA access on the same physical host. Suggested mitigations include IPsec to protect RDMA traffic, strict filtering and bounds checking of incoming RDMA traffic and using hardware support for I/O sharing such as Intel's V-T technology.

Security aspects of VM placement and inter-VM traffic routing have so far received relatively little attention. In particular, there are apparent trade-offs between mechanisms that focus on performance and approaches that take security concerns into account. For example, to improve performance one might co-locate closely interacting VMs, in order to reduce latency. However, to improve security the goal might be to strive for isolation of potentially co-harmful VMs.

Mikelangelo will reduce the attack surface of existing VM technology and of new features in sKVM. To mitigate side channel attacks, Mikelangelo will investigate mechanisms, on the hypervisor level. This approach will mitigate the effects of sharing physical resources with a malicious VM. Thus, Mikelangelo will reliably block known side-channels with the minimal possible effect on performance. The security system will provide this protection only to users that specifically require it. Mikelangelo will mitigate the effects of VM escapes by leveraging the network and other cloud components. To provide multi-tiered security, Mikelangelo will incorporate network security with VM placement and cloud monitoring.

IMPROVED SCALABILITY, USABILITY, AND SECURITY IN THE CLOUD: INTEGRATION OF A CLOUD MIDDLEWARE WITH SKVM AND OSV

Mikelangelo will integrate the advancements from the virtualisation layers with the cloud layer. The cloud layer consists of the infrastructure layer and the platform layer. This integration will make fast I/O, inter-VM communication, and improved security usable in cloud computing in practice. As a basis Mikelangelo will work with OpenStack as middleware for cloud computing. OpenStack found broad deployment and backing in industry and it has an open source license. These features make OpenStack the preferred choice for a cloud middleware in Mikelangelo. The following paragraphs describe how Mikelangelo will extend the infrastructure layer, the platform layer, and how it will integrate monitoring in the stack.

GWDG's Contributions in Mikelangelo

GWDG provides three main contributions in Mikelangelo:

1. Integration of the whole platform and deployment of a test bed.
2. Steering of all use case implementations.
3. Dissemination and evangelism of the project´s results.

In the infrastructure layer Mikelangelo will combine OpenStack to use sKVM for virtualisation in combination with OSv as preferred guest OS. Mikelangelo will extend OpenStack to incorporate the security considerations discussed in the previous section. This integration work primarily concerns itself with high performance and scalability. The work on sKVM and OSv provides the potential for high performance and improved scalability and elasticity. To harness this potential, Mikelangelo will need to integrate those technologies seamlessly into OpenStack. New bottlenecks will arise in OpenStack, which do not surface without sKVM and OSv. Engineers at GWDG will identify those bottlenecks and work to resolve them. Resolving bottlenecks and improving security in the cloud layer relates to resource allocation problems. Thus, GWDG engineers will research resource management algorithms, which satisfy security, privacy, performance end energy constraints. Furthermore, these algorithms will adapt to different circumstances. The cloud bursting module will feature this adaptivity, to detect cloud bursts quickly.

In the platform layer, Mikelangelo will integrate OSv's Capstan for simple application deployment. Capstan resembles Docker. However, Docker uses Linux containers instead of full virtualization. Capstan will instead use OSv and sKVM, to deploy applications easily. In the cloud layer, Mikelangelo will provide a web-based graphical user interface to deploy pre-packaged applications. Furthermore, the user interface will allow to manage and monitor those applications. The platform layer will also feature a simple and easy cloudification of applications based on Capstan. Thus, the application management component in the cloud layer will provide a reduced notion of a platform layer.

Mikelangelo will integrate monitoring as a cross-sectional concern in the cloud layer. This integration builds on previous work from Intel. Mikelangelo will work on currently open issues such as to research methods to describe metrics in a machine readable way. Metric descriptions need to cover aspects such as metric processing, dimensionality, and the origin of data. Furthermore, Mikelangelo will integrate monitoring metrics from all layers, starting with sKVM and progressing up to custom applications running via Capstan. To identify metrics that influence performance, Mikelangelo will deploy an automated analysis tool, developed by Intel.

USE CASES: BIG DATA, HPC, AND CLOUD

Four use cases in the three areas big data, HPC, and cloud computing drive the requirements, evaluation, and verification of Mikelangelo's stack. One use case uses Mikelangelo for applications in the context of big data. There are two use cases in the context of HPC. The fourth use case covers cloud bursting. We will introduce all four use cases briefly in the following paragraphs.

The big data use case will deploy a big data platform, such as Apache Hadoop, on Mikelangelo's cloud stack. Currently, big data applications do not lend themselves for execution on virtual infrastructure due to the high I/O overhead of current-generation VMs. However, running big data platforms in a cloud environment would have many benefits. Two important benefits are flexibility and agility. Flexibility means that in a virtualised big data cloud users could use a range of custom tools to run their analyses on large data sets. Agility means that users can deploy applications as required and when required onto the infrastructure. In this use case, GWDG will

integrate a big data platform that we will use Mikelangelo's cloud stack. Thus, GWDG aims to provide a productive big data cloud. Furthermore, in Mikelangelo GWDG plans to support users to port their applications to a big data framework. GWDG's users, in turn, will be able to execute these applications on Mikelangelo's stack on GWDG's infrastructure.

The first use case in high-performance computing deals with the simulation of cancellous bones. These simulations allow surgeons to develop better prostheses, such as hip-replacements. In practice, such a simulation increases the life-time of a hip replacement from ten years to multiples decades. Currently, programmers need to adapt such specific simulations to specific hardware and software, which includes the operating environment. This environment includes the operating system and available interfaces and programming libraries. Virtualisation will be a helpful tool, to allow users to provide their own flexible environment in VMs. However, currently virtualisation performs too poorly for I/O operations, to use virtualisation for HPC. In Mikelangelo, HLRS will port the cancellous bones simulation to OSv. Furthermore, HLRS will run OSv on sKVM with RDMA on an HPC cluster. This setup will give the users of the cancellous bones simulation, such as clinics, a way to run their simulation on a variety of computers. These computers can then easily involve, otherwise idle machine on users' premises.

The second HPC use case runs simulations in computational fluid dynamics with OpenFOAM. A Slovenian aircraft manufacturer called Pipistrel, uses these simulations to design new aircrafts. For Pipistrel it does not make sense to run their own HPC cluster, since their engineers require these simulations only periodically in some phases of aircraft design. Renting time on an HPC cluster also does not make sense, since Pipistrel's workflow requires a close interaction with the application. Often engineers run, evaluate, and then re-run designs with different parameters. Deploying OpenFOAM in a normal cloud built with the usual hardware setup also does not suffice, because OpenFOAM requires a fast interconnect. Thus, in Mikelangelo, Huawei and Pipistrel will port OpenFOAM to OSv and combine OpenFOAM with sKVM and RDMA. Furthermore, Huawei and Pipistrel will develop tools that will allow engineers to follow an agile workflow to quickly evaluate new aircraft designs.

The cloud bursting use case aims to deal with bursts of requests of internet services better. Cloud bursts are an internet phenomenon that happens regularly. A cloud burst appears when a large number of users suddenly request some resources or when they try to use a service. Then, scaling mechanisms usually deploy new VMs to cope with the high demand. However, often such a burst reaches the limits of the infrastructure very quickly. There are two important metrics that drive how well a cloud handles cloud bursts: transfer times for VM images and boot time for VMs. OSv shines in both categories. Since Cloudius Systems has designed OSv from scratch, the operating system's VM image has a size of only a few MBs. Start-up times of OSv usually lie under a second. In this use case, Cloudius will take advantage of OSv and fast I/O with sKVM and RDMA, to distribute applications very quickly. In specific, these applications will carry state, which will be transferred to the freshly deployed VMs.

CONCLUSIONS

Mikelangelo provides a well-balanced mixture regarding expertise, organisational background, and technological maturity. This mixture allows the project to provide a robust system with crucial novelties. The key results are an improved version of KVM, an optimised operating system for the cloud, new RDMA methods, improved security for VMs, and new application deployment methods. Furthermore, Mikelangelo will apply those advancements to cloud computing and HPC.

The project has just begun with a kick-off meeting. Now the consortium collects requirements to design the initial system architecture. During the upcoming months GWDG and HLRS will set up test beds for the project. These test beds will serve as reference for all implementations in the project. Furthermore, the test beds will allow use cases to benchmark their applications to obtain an initial performance baseline.

We will provide updates on the project status throughout the project duration in GWDG News. For current news, please visit our web site (*http://www.mikelangelo-project.eu*) and follow us on Twitter (*mikelangelo_eu*) and LinkedIn (*mikelangelo_eu*).

If you have a large data set, and if you are interested to become an early adaptor of novel technogies by contributing a big data use case, please contact the author.

ACKNOWLEDGEMENT

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645402.

Personalia

NEUER MITARBEITER HANS HENNING THIES

Seit dem 1. Februar 2015 unterstützt Herr Hans Henning Thies die Arbeitsgruppe „Nutzerservice und Betriebsdienste“ (AG H) im Bereich der SharePoint-Administration mit dem Schwerpunkt auf der SharePoint-Umgebung der Generalverwaltung der Max-Planck-Gesellschaft. Herr Thies war zuvor mehrere Jahre im Soziologischen Forschungsinstitut Göttingen (SOFI) als Systemadministrator und IT-Fachkraft tätig. Er ist per E-Mail unter *hans-henning.thies@gwdg.de* und telefonisch unter 0551 201-1833 erreichbar.

Heuer

NEUER MITARBEITER KHAWAR MUNIR ABBASI

Seit dem 1. Februar 2015 verstärkt Herr Khawar Munir Abbasi die Arbeitsgruppe „eScience“ (AG E) im Bereich Software Defined Networking. Er arbeitet an dem Projekt NEPHELE mit, welches von der Europäischen Union gefördert wird und sich mit Fragen der Integration and Verbesserung von Netzwerktechnologien in zunehmend virtualisierten Rechenzentren befasst. Herr Abbasi hat einen Masterabschluss in Computer/Communication Engineering der RWTH Aachen und bringt umfassende Erfahrung aus dem Netzwerkbereich und aus dem Cloud-Umfeld mit. Zudem war Herr Abbasi auch operativ und in der Softwareentwicklung in Industrieunternehmen tätig. Wir freuen uns über die Verstärkung in dem für die GWDG und seine Kunden zukunftsweisenden Forschungsgebiet. Herr Abbasi ist per E-Mail unter *khawar-munir.abbasi@gwdg.de* und telefonisch unter 0551 39-21107 erreichbar.

Wieder

NEUE MITARBEITERIN MARTINA BRÜCHER

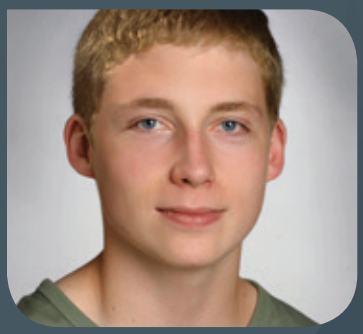
Seit dem 16. Februar 2015 wird die Arbeitsgruppe „eScience“ (AG E) durch eine neue Mitarbeiterin unterstützt: Frau Martina Brücher übernimmt administrative Aufgaben im Forschungsprojektumfeld der GWDG. Frau Brücher hat ihr Studium der Rechtswissenschaften an der Georg-August-Universität Göttingen 1993 abgeschlossen und 1996 das „2. juristische Staatsexamen“ erworben. Bereits während des Referendariats spezialisierte sie sich auf Tätigkeiten in der öffentlichen Verwaltung. Frau Brücher bringt Berufserfahrungen aus verschiedenen öffentlichen Einrichtungen mit und richtet ihr Augenmerk insbesondere auf interdisziplinäre Zusammenarbeit, administrative Projektunterstützung und Qualitätsmanagement. Zudem bringt sie ihre Erfahrungen aus den Bereichen Wissensmanagement und Change Management in die Arbeitsgruppe „eScience“ mit ein. Frau Brücher ist per E-Mail unter *martina.bruecher@gwdg.de* erreichbar.

Wieder

NEUE MITARBEITERIN MARIANA SLAV

Seit dem 1. Februar 2015 wird die Verwaltung der GWDG durch eine neue Mitarbeiterin unterstützt: Frau Mariana Slav übernimmt vorübergehend unterstützende Aufgaben in der Verwaltung. Frau Slav hat 2014 ihr Bachelor-Studium der Betriebswirtschaftslehre an der Georg-August-Universität Göttingen abgeschlossen. Ihre Studienschwerpunkte lagen in den Bereichen Marketing, Steuern und Unternehmensführung. Frau Slav ist telefonisch unter 0551 201-1531 und per E-Mail unter *mariana.slav@gwdg.de* erreichbar.

Suren



AUSBILDUNG ERFOLGREICH ABGESCHLOSSEN
ROBIN KLEINHANS UND JANNIK RICHTER

Herr Robin Kleinhans und Herr Jannik Richter haben am 23. Januar 2015 ihre Abschlussprüfung zum Elektroniker für Geräte und Systeme mit guten Ergebnissen bestanden und damit ihre 3,5-jährige Ausbildung bei der GWDG erfolgreich beendet. Im Anschluss an ihre Ausbildung werden die neuen Facharbeiter bei der GWDG weiterbeschäftigt. Sie werden sich vor allem mit der Installation von Hardware im Maschinenraum und der TP-Verkabelung der Mitarbeiterbüros befassen. Herr Kleinhans hat die GWDG zum 1. März 2015 verlassen. Wir wünschen ihm für seinen weiteren beruflichen wie privaten Lebensweg viel Erfolg und alles Gute.

Gutsch

GWDG
Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

Using the Parallel Processing Power of the GWDG Scientific Compute Cluster

Upcoming Introductory and Parallel Programming Courses

GWDG operates a scientific compute cluster with currently 17,900 cores and a total compute power of 250 Teraflops ($2.5*10^{14}$ floating point operations per second), which can be used by all scientists of the institutes of GWDG's supporting organisations, University of Göttingen and Max Planck Society.

In order to facilitate the access to and the efficient use of these computing resources, GWDG offers introductory and parallel programming courses, held at GWDG's site 'Am Faßberg'.

The next courses in 2015 are

> March 30th, 9:30 am - 4:00 pm

Using the GWDG Scientific Compute Clusters – an Introduction

This course explains all steps for accessing GWDG's clusters, to compile and install software, and to work with the batch system for the execution of application jobs. The course is intended for new or inexperienced users of the clusters.

> March 31th - April 1st, 9:15 am - 5:00 pm

Parallel Programming with MPI (Including MPI for Python)

This course introduces the message passing interface (MPI) for programming parallel applications in FORTRAN, C, and in Python. All concepts will be illustrated with hands on exercises. Examples of parallel applications will be presented and analysed.

> May 7th, 9:15 am - 4:30 pm

High-level, High-performance Technical Computing with Julia

Julia is a modern programming language combining high-level dynamic programming with high performance. The course covers the basics of Julia including numerical computing, parallel computing, and statistical methods.

These three courses are repeated regularly. Other courses on parallel computing, dealing with more specialized topics can be arranged on demand. The possible subjects include parallel programming for shared memory systems and for graphics processors, and using extensions of C or Fortran with high level parallel constructs.

More Information about the courses held regularly or on demand at *www.gwdg.de/scientific-computing-courses*.

Information for registering for the courses at *www.gwdg.de/courses*.

If you have any further questions please contact *support@gwdg.de*.

www.gwdg.de/courses

INFORMATIONEN:
support@gwdg.de
0551 201-1523

März bis Dezember 2015

Kurse

KURS	VORTRAGENDE/R	TERMIN	ANMELDEN BIS	AE
INSTALLATION UND ADMINISTRATION VON WINDOWS 7	Buck	11.03.2015 9:00 – 12:30 und 13:30 – 15:30 Uhr	04.03.2015	4
PHOTOSHOP FÜR FORTGESCHRITTENE	Töpfer	16.03. – 17.03.2015 9:30 – 16:00 Uhr	09.03.2015	4
USING THE GWDG SCIENTIFIC COMPUTE CLUSTER – AN INTRODUCTION	Dr. Boehme	30.03.2015 9:30 – 16:00 Uhr	23.03.2015	4
PARALLELRECHNERPROGRAMMIERUNG MIT MPI	Prof. Haan	31.03. – 01.04.2015 9:15 – 17:00 Uhr	24.03.2015	8
INDESIGN – AUFBAUKURS	Töpfer	13.04. – 14.04.2015 9:30 – 16:00 Uhr	06.04.2015	8
OUTLOOK – E-MAIL UND GROUPWARE	Helmvoigt	16.04.2015 9:15 – 12:00 und 13:00 – 16:00 Uhr	09.04.2015	4
EINFÜHRUNG IN DIE STATISTISCHE DATENANALYSE MIT SPSS	Cordes	22.04. – 23.04.2015 9:00 – 12:00 und 13:00 – 15:30 Uhr	15.04.2015	8
ADMINISTRATION VON PCS IM ACTIVE DIRECTORY DER GWDG	Buck	29.04.2015 9:00 – 12:30 und 13:30 – 15:30 Uhr	22.04.2015	4
UNIX FÜR FORTGESCHRITTENE	Dr. Sippel	04.05. – 06.05.2015 9:15 – 12:00 und 13:15 – 15:30 Uhr	27.04.2015	12
HIGH-LEVEL, HIGH-PERFORMANCE TECHNICAL COMPUTING WITH JULIA	Chronz	07.05.2015 9:15 – 16:30 Uhr	30.04.2015	4

KURS	VORTRAGENDE/R	TERMIN	ANMELDEN BIS	AE
MAC OS X IM WISSENSCHAFTLICHEN ALLTAG	Bartels	12.05. – 13.05.2015 9:30 – 16:30 Uhr	05.05.2015	8
EINFÜHRUNG IN DAS IP-ADRESSMANAGEMENTSYSTEM DER GWDG FÜR NETZWERKBEAUFTRAGTE	Dr. Beck	19.05.2015 10:00 – 12:00 Uhr	12.05.2015	2
ANGEWANDTE STATISTIK MIT SPSS FÜR NUTZER MIT VORKENNTNISSEN	Cordes	20.05. – 21.05.2015 9:00 – 12:00 und 13:00 – 15:30 Uhr	13.05.2015	8
DIE SHAREPOINT-UMGEBUNG DER GWDG	Buck	03.06.2015 9:00 – 12:30 und 13:30 – 15:30 Uhr	27.05.2015	4
QUICKSTARTING R: EINE ANWENDUNGSORIENTIERTE EINFÜHRUNG IN DAS STATISTIKPAKET R	Cordes	17.06. – 18.06.2015 9:00 – 12:00 und 13:00 – 15:30 Uhr	10.06.2015	8
DATENSCHUTZ – VERARBEITUNG PERSONENBEZOGENER DATEN AUF DEN RECHENANLAGEN DER GWDG	Dr. Grieger	24.06.2015 9:00 – 12:00 Uhr	17.06.2015	2
HIGH-LEVEL, HIGH-PERFORMANCE TECHNICAL COMPUTING WITH JULIA	Chronz	07.09.2015 9:15 – 16:30 Uhr	31.08.2015	4
EINFÜHRUNG IN WINDOWS 8	Buck	09.09.2015 9:00 – 12:30 Uhr	02.09.2015	2
GRUNDLAGEN DER BILDBEARBEITUNG MIT PHOTOSHOP	Töpfer	14.09. – 15.09.2015 9:30 – 16:00 Uhr	07.09.2015	8
DIE SHAREPOINT-UMGEBUNG DER GWDG	Buck	23.09.2015 9:00 – 12:30 und 13:30 – 15:30 Uhr	16.09.2015	4
INDESIGN – GRUNDLAGEN	Töpfer	28.09. – 29.09.2015 9:30 – 16:00 Uhr	21.09.2015	8
INSTALLATION UND ADMINISTRATION VON WINDOWS 8	Buck	07.10.2015 9:00 – 12:30 und 13:30 – 15:30 Uhr	30.09.2015	4
PHOTOSHOP FÜR FORTGESCHRITTENE	Töpfer	02.11. – 03.11.2015 9:30 – 16:00 Uhr	26.10.2015	8
OUTLOOK – E-MAIL UND GROUPWARE	Helmvoigt	05.11.2015 9:15 – 12:00 und 13:00 – 16:00 Uhr	29.10.2015	4
ADMINISTRATION VON PCS IM ACTIVE DIRECTORY DER GWDG	Buck	09.11.2015 9:00 – 12:30 und 13:30 – 15:30 Uhr	02.11.2015	4
EINFÜHRUNG IN DIE STATISTISCHE DATENANALYSE MIT SPSS	Cordes	11.11. – 12.11.2015 9:00 – 12:00 und 13:00 – 15:30 Uhr	04.11.2015	8
INDESIGN – AUFBAUKURS	Töpfer	16.11. – 17.11.2015 9:30 – 16:00 Uhr	09.11.2015	8

KURS	VORTRAGENDE/R	TERMIN	ANMELDEN BIS	AE
EINFÜHRUNG IN DAS IP-ADRESSMANAGEMENTSYSTEM DER GWDG FÜR NETZWERKBEAUFTRAGTE	Dr. Beck	18.11.2015 10:00 – 12:00 Uhr	11.11.2015	2
QUICKSTARTING R: EINE ANWENDUNGSORIENTIERTE EINFÜHRUNG IN DAS STATISTIKPAKET R	Cordes	25.11. – 26.11.2015 9:00 – 12:00 und 13:00 – 15:30 Uhr	18.11.2015	8
UNIX FÜR FORTGESCHRITTENE	Dr. Sippel	30.11. – 02.12.2015 9:15 – 12:00 und 13:15 – 15:30 Uhr	23.11.2015	12
HIGH-LEVEL, HIGH-PERFORMANCE TECHNICAL COMPUTING WITH JULIA	Chronz	03.12.2015 9:15 – 16:30 Uhr	26.11.2015	4
ANGEWANDTE STATISTIK MIT SPSS FÜR NUTZER MIT VORKENNTNISSEN	Cordes	09.12. – 10.12.2015 9:00 – 12:00 und 13:00 – 15:30 Uhr	02.12.2015	8
DIE SHAREPOINT-UMGEBUNG DER GWDG	Buck	16.12.2015 9:00 – 12:30 und 13:30 – 15:30 Uhr	09.12.2015	4

Teilnehmerkreis
Das Kursangebot der GWDG richtet sich an alle Mitarbeiterinnen und Mitarbeiter aus den Instituten der Universität Göttingen und der Max-Planck-Gesellschaft sowie aus einigen anderen wissenschaftlichen Einrichtungen.

Anmeldung
Anmeldungen können schriftlich per Brief oder per Fax unter der Nummer 0551 201-2150 an die GWDG, Postfach 2841, 37018 Göttingen oder per E-Mail an die Adresse *support@ gwdg.de* erfolgen. Für die schriftliche Anmeldung steht unter *http://www.gwdg.de/antragsformulare* ein Formular zur Verfügung. Telefonische Anmeldungen können leider nicht angenommen werden.

Kosten bzw. Gebühren
Unsere Kurse werden wie die meisten anderen Leistungen der GWDG in Arbeitseinheiten (AE) vom jeweiligen Institutskontingent abgerechnet. Für die Institute der Universität Göttingen und der Max-Planck-Gesellschaft erfolgt keine Abrechnung in EUR.

Absage
Sie können bis zu acht Tagen vor Kursbeginn per E-Mail an *support@gwdg.de* oder telefonisch unter 0551 201-1523 absagen. Bei späteren Absagen werden allerdings die für die Kurse berechneten AE vom jeweiligen Institutskontingent abgebucht.

Kursorte
Alle Kurse finden im Kursraum oder Vortragsraum der GWDG statt. Die Wegbeschreibung zur GWDG sowie der Lageplan sind unter *http://www.gwdg.de/lageplan* zu finden.

Kurstermine
Die genauen Kurstermine und -zeiten sowie aktuelle kurzfristige Informationen zu den Kursen, insbesondere zu freien Plätzen, sind unter *http://www.gwdg.de/kurse* zu finden.


GWDG
Gesellschaft für wissenschaftliche
Datenverarbeitung mbH Göttingen