Gesellschaft für Informatik (GI)

publishes this series in order to make available to a broad public recent findings in informatics (i.e. computer science and information systems), to document conferences that are organized in cooperation with GI and to publish the annual GI Award dissertation.

Broken down into the fields of
- Seminars
- Proceedings
- Dissertations
- Thematics

current topics are dealt with from the fields of research and development, teaching and further training in theory and practice. The Editorial Committee uses an intensive review process in order to ensure the high level of the contributions.

The volumes are published in German or English.

Information: http://www.gi-ev.de/service/publikationen/lni/

ISSN 1617-5468
ISBN 978-3-88579-260-4

The 3. DFN-Forum Communication Technologies 2010 is taking place in Constance, Germany, from Mai 26th to Mai 27th.

This volume contains 12 papers selected for presentation at the conference.

To assure scientific quality, the selection was based on a strict and anonymous reviewing process.

Paul Müller, Bernhard Neumair, Gabi Dreo Rodosek (Hrsg.): 3. DFN-Forum 2010

166

GI-Edition

Lecture Notes in Informatics

Paul Müller, Bernhard Neumair, Gabi Dreo Rodosek (Hrsg.)

3. DFN-Forum Kommunikations-technologien

Beiträge der Fachtagung

26. Mai bis 27. Mai 2010
Konstanz

Proceedings

Paul Müller, Bernhard Neumair, Gabi Dreo Rodosek (Hrsg.)

3. DFN-Forum Kommunikationstechnologien

Verteilte Systeme im Wissenschaftsbereich

26.05. - 27.05.2010
in Konstanz

Gesellschaft für Informatik e.V. (GI)

Lecture Notes in Informatics (LNI) - Proceedings
Series of the Gesellschaft für Informatik (GI)

Volume P-166

ISBN 978-3-88579-260-4
ISSN 1617-5468

Volume Editors
Prof. Dr. Paul Müller
Technische Universität Kaiserslautern
Postfach 3049, 67653 Kaiserslautern
Email: pmueller@informatik.uni-kl.de
Prof. Dr. Bernhard Neumair
Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen
Am Fassberg, 37077 Göttingen
Email: Bernhard.Neumair@gwdg.de
Prof. Dr. Gabi Dreo Rodosek
Universität der Bundeswehr München
Werner-Heisenberg-Weg 39, 85577 Neubiberg
Email: Gabi.Dreo@unibw.de

printed by Köllen Druck+Verlag GmbH, Bonn

Vorwort

Der DFN-Verein ist seit seiner Gründung dafür bekannt, neueste Netztechnologien und innovative netznahe Systeme einzusetzen und damit die Leistungen für seine Mitglieder laufend zu erneuern und zu optimieren. Beispiele dafür sind die aktuelle Plattform des Wissenschaftsnetzes X-WiN und Dienstleistungen für Forschung und Lehre wie die DFN-PKI und DFN-AAI. Um diese Technologien einerseits selbst mit zu gestalten und andererseits frühzeitig die Forschungsergebnisse anderer Wissenschaftler kennenzulernen, veranstaltet der DFN-Verein seit vielen Jahren wissenschaftliche Tagungen zu Netztechnologien. Mit den Zentren für Kommunikation und Informationsverarbeitung in Forschung und Lehre (ZKI) e.V. und der Gesellschaft für Informatik e.V. (GI) gibt es in diesem Bereich eine langjährige und fruchtbare Zusammenarbeit.

Das 3. DFN-Forum Kommunikationstechnologien „Verteilte Systeme im Wissenschaftsbereich“ steht in dieser Tradition. Nach den beiden sehr erfolgreichen Vorgängerveranstaltungen in den Jahren 2008 und 2009 in Kaiserslautern und München wird die diesjährige Tagung vom DFN-Verein und der Universität Konstanz gemeinsam mit dem ZKI e.V. und der GI am 26. und 27. Mai 2010 in Konstanz veranstaltet und soll eine Plattform zur Darstellung und Diskussion neuer Forschungs- und Entwicklungsergebnisse aus dem Bereich TK/IT darstellen. Das Forum dient dem Erfahrungsaustausch zwischen Wissenschaftlern und Praktikern aus Hochschulen, Großforschungseinrichtungen und Industrie.

Aus den eingereichten Beiträgen konnte ein hochwertiges und aktuelles Programm zusammengestellt werden, das neben künftigen Netztechnologien unter anderem auf Grid- und Cloud-Technologien, Identity Management und IT-Sicherheit eingeht. Ergänzt wird es durch eine Podiumsdiskussion zu Outsourcing-Fragen in der wissenschaftlichen IT und durch eingeladene Beiträge zu Virtualisierungstechnologien, zu Großprojekten im High-Performance-Computing wie DEISA und PRACE und deren Auswirkungen auf die künftige HPC-Versorgung in Deutschland und zur Mobilität von Wissenschaftlerinnen und Wissenschaftlern und den daraus resultierenden Nutzungsszenarien künftiger Netze. Um den Rahmen der Veranstaltung nicht zu sprengen, konnten leider nur weniger als die Hälfte der eingereichten Beiträge angenommen werden. Dies zeigt, dass die Veröffentlichung der Beiträge sowohl im Rahmen der GI-Edition Lecture

Notes in Informatics als auch mit Open Access für die Wissenschaftlerinnen und Wissenschaftler attraktiv ist.

Wir möchten uns bei den Autoren für alle eingereichten Beiträge, beim Programmkomitee für die Auswahl der Beiträge und die Zusammenstellung des Programms und bei den Mitarbeiterinnen und Mitarbeitern für die umfangreichen organisatorischen Arbeiten bedanken. Allen Teilnehmern wünschen wir für die Veranstaltung interessante Vorträge und fruchtbare Diskussionen.

Konstanz, Mai 2010

Paul Müller
Bernhard Neumair
Gabi Dreo Rodosek

Programmkomitee

Alexander Clemm, Cisco

Gabi Dreo Rodosek (Co-Chair), Universität der Bundeswehr München

Thomas Eickermann, Forschungszentrum Jülich

Markus Fidler, Universität Hannover

Alfred Geiger, T-Systems SfR

Wolfgang Gentzsch, DEISA

Hannes Hartenstein, KIT

Dieter Hogrefe, Universität Göttingen

Eike Jessen, Technische Universität München

Ulrich Lang, Universität zu Köln

Paul Müller (Co-Chair), Technische Universität Kaiserslautern

Bernhard Neumair (Co-Chair), Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

Gerhard Peter, Hochschule Heilbronn

Christa Radloff, Universität Rostock

Helmut Reiser, LRZ München

Peter Schirmbacher, Humboldt-Universität, Berlin

Uwe Schwiegelshohn, Universität Dortmund

Manfred Seedig, Universität Kassel

Marcel Waldvogel, Universität Konstanz

René Wies, BMW Group

Inhaltsverzeichnis

Grid & Cloud Computing

Erweiterung einer D-Grid Ressource um eine Compute Cloud Schnittstelle

Stefan Freitag

stefan.freitag@tu-dortmund.de

Abstract: Das D-Grid Ressourcen Zentrum Ruhr (DGRZR) stellt den D-Grid Communities seit 2008 monatlich Rechenkapazität in Höhe von 1,4 Mio. CPUh zur Verfügung. Im Vergleich mit vielen anderen D-Grid Ressourcen hebt sich das DGRZR durch zwei Besonderheiten hervor: i) alle betriebenen Dienste sind in virtuelle Maschinen gekapselt und ii) lehnt sich die Installation sehr nah an die durch D-Grid vorgeschlagene Referenzinstallation an.
Beide Punkte begünstigten die prototypische Erweiterung des DGRZR um Cloud Middleware Schnittstellen. Diese Erweiterung des DGRZR sowie gesammelte Erfahrungen werden in dieser Arbeit beschrieben. Weiterführend werden fehlende Komponente für die Integration der neuen Schnittstelle in das D-Grid identifiziert und erste Lösungsansätze präsentiert.

1 Einleitung

Das D-Grid Ressourcen Zentrum Ruhr (DGRZR) stellt dem D-Grid seit 2008 Rechen- sowie Speicherressourcen in Höhe von ca. 2.000 Cores bzw. 100 TByte Massenspeicher zur Verfügung. Der Zugriff seitens D-Grid erfolgt über die Grid Middlewares gLite 3.1 [1], Globus Toolkit 4 [2] und UNICORE5 bzw. UNICORE6 [3]. Weiterhin ist das DGRZR durch zwei Besonderheiten charakterisiert: i) alle bereitgestellten Dienste sind in virtuelle Maschine gekapselt und ii) lehnt sich die Installation stark an die durch D-Grid vorgeschlagene Referenzinstallation [4] an. Beide Punkte begünstigten die prototypische Erweiterung des DGRZR um Cloud Middleware Schnittstellen.
Nachfolgend werden existierende Arbeiten in dem Themenbereich vorgestellt. Abschnitt 3 stellt Cloud Computing in verschiedenen Ausprägungen vor. Die bisherigen Arbeiten am DGRZR zur Zusammenführung von Grid und Cloud Computing auf einer D-Grid Ressource sind in Abschnitt 4 beschrieben. Im Anschluss daran präsentiert Abschnitt 5 offene Arbeiten zur Integration des Cloud Schnittstelle in das D-Grid.

[1] http://glite.web.cern.ch/glite/
[2] http://www.globus.org/toolkit/
[3] http://www.unicore.eu/
[4] http://dgiref.d-grid.de/wiki/Introduction

2 Existierende Arbeiten

Die Installation und der Betrieb von Grid Middleware Diensten in einer Compute Cloud stellt eines der aktuell untersuchten Szenarien dar [Llo09], wobei drei Varianten erkennbar sind. Variante 1 beschäftigt sich mit der dynamischen Bereitstellung von Workernodes in der privaten Compute Cloud des Betreibers. Diese Workernodes – implementiert als virtuelle Maschinen – integrieren sich automatisch in das LRMS (Local Resource Management System) und stehen anschließend für die Jobabarbeitung zur Verfügung. Reichen die physischen Ressourcen des Compute Cloud Betreibers nicht aus, nimmt dieser in Variante 2 Kapazitäten anderer Compute Clouds in Anspruch, um auf diesen weitere Workernodes zu starten. Nach dem Start integrieren sich die Workernodes wie in Variante 1 in das LRMS des Betreibers. Variante 3 entspricht Situationen, in denen nicht nur einzelne Knoten bzw. Dienste dynamisch in einer Cloud starten, sondern eine vollständige Grid Site.
Des Weiteren existieren im Bereich des Cloud Computing erste Arbeiten [Buy09] hinsichtlich einer Orchestrierungsschicht, wie es sie im Grid Computing seit langem gibt. In dieser Schicht werden u.a. Informationen zu verschiedenen Compute Cloud Anbietern (z. B. Kosten pro CPUh, Verfügbarkeit) aggregiert und nach außen verfügbar gemacht. Ein Profiteur dieser Informationen ist der Prozess des Matchmaking zwischen den Anforderungen des Kunden und den verfügbaren Ressourcen.
Analog zu der Entwicklung von libvirt [5] gibt es mit libcloud [6] eine prototypische API, die Schnittstellen zu verschiedenen Compute Clouds (z.B. Amazon EC2 [7] oder Rackspace) kapselt. Nachdem vielerorts EC2 für Compute Clouds als Quasi-Standard Schnittstelle angesehen wird, ist mit OCCI [Edm09] die Bestrebung hin zur Definition eines echten Standards erkennbar.

3 Cloud Computing

Cloud Computing ist im IT-Umfeld eine der sich derzeit am schnellsten ausbreitenden Technologien. Der vor ca. zwei Jahren einsetzende Hype um dieses Thema ist durch kontinuierlich steigendes Anfrageaufkommen an Suchmaschinen belegbar (vgl. Abbildung 1) Wie dem Grid Computing fehlt auch dem Cloud Computing eine allgemein akzeptierte Definition. In [Vaq09] wurden verschiedene Cloud Definitionen herangezogen und mit Skalierbarkeit, Virtualisierung und dem Pay-Per-Use Modell drei Merkmale identifiziert, die in vielen der Definitionen vorkamen.

Seit seinem ersten Erscheinen wurde die Verbreitung und Weiterentwicklung des Cloud Computing durch kommerzielle Anbieter forciert. Diese öffnen ihre Ressourcen über Compute und/ oder Storage Cloud Schnittstellen für Fremdnutzer und erzielen somit i) eine gesteigerte Auslastung und ii) über das Pay-Per-Use Geschäftsmodell Mehreinnahmen.
Derzeit existierende Clouds sind in Abhängigkeit der von ihnen angebotenen Dienste in drei Kategorien einteilbar, die nachfolgend kurz vorgestellt werden.

[5] http://libvirt.org/
[6] http://incubator.apache.org/libcloud/
[7] http://aws.amazon.com/ec2/

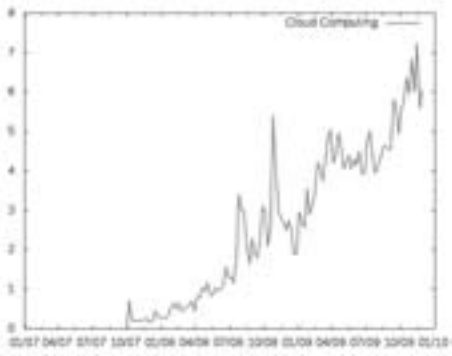


Abbildung 1: Google Trends Ergebnisse zu Cloud Computing (Stand: 09.12.2009, Quelle: http://www.google.de/trends). Die Werte auf der y-Achse reflektieren den Quotienten Suchverkehr für den Suchbegriff/ Durchschnittlicher Suchverkehr.

Infrastructure-as-a-Service (IaaS) Über Schnittstellen wie EC2 oder OCCI fordern Kunden die Bereitstellung von z. B. Virtual Appliances oder Speicher an und verschalten diese Ressourcen zur benötigten Infrastruktur.

Platform-as-a-Service (PaaS) Kunden erhalten bei PaaS Anbietern Zugriff auf Software Plattformen (z. B. Google Apps Engine [8]). Auf diesen Plattformen entwickeln Kunden eigene Dienste und greifen bei Bedarf auf Werkzeuge des PaaS Anbieters zurückgreifen.

Software-as-a-Service (SaaS) SaaS Kunden greifen über das Internet auf Software zu, die in einer Cloud betrieben wird. Ein Beispiel hierfür ist GoogleDocs [9], welches u. a. eine Anwendung zur Textverarbeitung anbietet.

4 Zusammenführung von Grid und Cloud am DGRZR

Wie in Abschnitt 2 beschrieben, fokussieren sich die aktuellen Anstrengungen auf das Deployment von Grid Middleware in Compute Clouds und auf die Konstruktion eines Grid of Clouds. Im Rahmen des noch jungen D-Grid [10] erscheint die Verbindung der Konzepte des Cloud und Grid Computing in ein uniformes Modell für das Angebot von Rechen- und Speicherressourcen erstrebenswert.

Nutzer erhalten einhergehend mit dem Zugriff über die Compute Cloud Schnittstelle eine einfache Möglichkeit selbsterstellte Software Appliances auf D-Grid Ressourcen auszuführen. Da die Software gekapselt in der Appliance läuft, ist sie unabhängig von der durch die Ressource bereitgestellten Umgebung (z. B. Bibliotheken und Compiler)[11].

[8] http://code.google.com/intl/de/appengine/
[9] http://docs.google.com
[10] http://www.d-grid.de
[11] Das aktuelle Fehlen eines common production environments in D-Grid führt zudem dazu, dass die bereitge-

Die Erweiterung des D-Grid Portfolios um eine EC2-kompatible Cloud Schnittstelle ermöglicht Anwendern zudem einen reibungslosen Umstieg von Fremdanbietern auf D-Grid. Gerade für KMU ist dies interessant, sie schrecken aufgrund der Komplexität der Grid Middlewares und zugehöriger Nutzerschnittstellen oftmals vor der Verwendung der D-Grid Ressourcen zurück.

Mit diesen Perspektiven in Aussicht wurde die D-Grid Ressource DGRZR um eine Cloud Middleware erweitert. Voraussetzung für die Erweiterung war die bereits existierende Kapselung der betriebenen Dienste in virtuelle Maschinen. Dies gilt insbesondere für die Grid Middleware Dienste von gLite, Globus Toolkit und UNICORE sowie dCache und OGSA-DAI. Die Plattform Virtualisierung beruht am DGRZR auf einem Mischbetrieb aus VMware 4 und Xen 3.2.3.
Abbildung 2 skizziert die schichtweise Anordnung der Dienste im DGRZR unter Berücksichtigung der hinzugekommenen Cloud Middleware, welche auf der Virtualisierungsschicht aufsetzt. Derzeit ist OpenNebula [12] 1.4 RC2 als Cloud Middleware am DGRZR

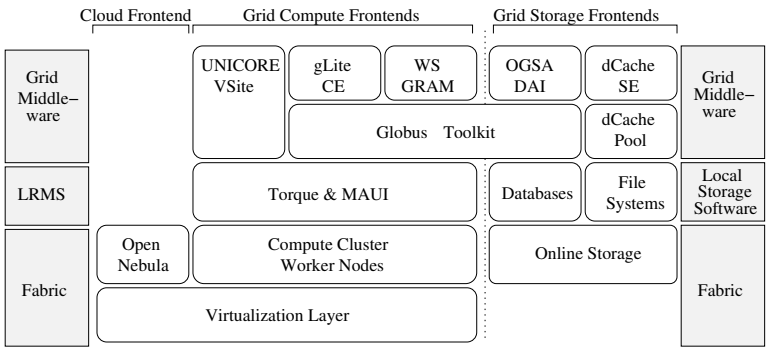


Abbildung 2: Schaubild der aktuellen Architektur des DGRZR

installiert. Anwender können virtuelle Appliances über die EC2 oder OCCI Schnittstelle registrieren, starten und stoppen. Der OpenNebula Daemon *oned* überwacht die virtuellen Appliances und prüft dazu periodisch ihren Status. Abbildung 3 zeigt die Ausgabe des Aufrufs *onevm list*, der eine Übersicht über die aktiven virtuellen Appliances auf dem Bildschirm ausgibt. Neben dem Status und dem reservierten Hauptspeicher ist für jede Appliance auch der Name des physischen Rechners, auf dem sie läuft, aufgeführt. Virtual Appliances, die nicht in OpenNebula registriert wurden, finden keine Berücksichtigung bei der Erstellung der Übersicht.

Aufgrund des Release Candidate Status von OpenNebula ist die Funktionalität der OCCI und EC2 Schnittstelle noch nicht vollständig implementiert.

stellte Umgebung Ressourcen-abhängig stark variieren kann.

[12] http://www.opennebula.org

ID	USER	NAME	STAT	CPU	MEM	HOSTNAME	TIME
16	oneadmin	centos.5	runn	0	262144	udo-bl1107	10 19:47:33
17	oneadmin	ubuntu9	runn	0	262144	udo-bl1106	10 19:42:26
18	oneadmin	debian.5	runn	0	262144	udo-bl2313	10 14:17:47

Abbildung 3: Ausgabe des Kommandos *onevm list*

5 Offene Arbeiten

Die Erfahrungen aus dem Betrieb und die vollständige Integration des DGRZR in das D-Grid ermöglichen die Identifikation offener Arbeiten für i) den Betrieb von Cloud und Grid Schnittstellen auf einer Ressource und ii) die Zusammenarbeit der Cloud Middleware OpenNebula mit den zentralen D-Grid Diensten. Im den folgenden Abschnitten steht vor allem der zweite Punkt im Vordergrund, wobei Problembereiche adressiert und mögliche Lösungswege aufgezeigt werden.

5.1 Nutzerverwaltung und Authentifikation

OpenNebula speichert Nutzer in einer zentralen SQLite3 Datenbank und unterteilt sie in zwei Kategorien: i) den super user *oneadmin* und ii) die restlichen, regulären Nutzer. Letztere dürfen nur selbstregistrierte Appliances und Netzwerke verwalten und müssen zuvor durch *oneadmin* angelegt werden. Als super user verwaltet *oneadmin* alle Objekte (Virtual Appliances, Netzwerke, Hosts und Nutzer).
Bevor das Kommando eines Nutzers (z. B. *econe-upload* zum Hochladen einer Virtual Appliance in die Cloud) ausgeführt wird, erfolgt eine Authentifikation. Grundlage der Authentifikation bilden die mit dem Kommando übergebenen Werte für *access key* und *secret key*. *access key* entspricht dem Nutzernamen, wie er durch *oneadmin* erzeugt wurde, und *secret key* einem Passwort, welches der Nutzer festgelegt hat. Gibt es in der SQLite3 Datenbank keine Entsprechung für *access key*, wird die Ausführung des Kommandos abgelehnt. Festzuhalten ist hierbei, dass für einen OpenNebula Nutzer kein lokales Konto auf der Ressource existieren muss.

Im Gegensatz zu OpenNebula erfolgt bei den am DGRZR unterstützten Grid Middlewares die Nutzerverwaltung nicht über eine Datenbank auf der Ressource selbst, sondern über den VOMRS (Virtual Organization Membership Registration Service), der einen zentralen Dienst innerhalb einer virtuellen Organisation [Fos01] darstellt. Mitglieder einer virtuellen Organisation werden über Mechanismen der Grid Middleware auf lokale Nutzerkonten auf der Ressource abgebildet.
Für die Authentifikation gibt es anhängig von der Grid Middleware unterschiedliche Verfahren. Beim Globus Toolkit kommt ein grid-mapfile zum Einsatz, welches die Abbildung des Grid Nutzers auf ein lokales Konto der Ressource enthält. Listing 1 zeigt exemplarisch einen Ausschnitt aus einem solchen grid-mapfile, wobei links der Distinguished Name aus dem X.509 Zertifikat des Grid Nutzers zu erkennen ist und rechts das lokale Nutzerkonto.

Listing 1: /etc/grid-security/grid-mapfile

```
1 "/C=DE/O=GermanGrid/OU=TU–Dortmund/CN=XXXXXX XXXXXX" dt0061
2 "/C=DE/O=GermanGrid/OU=TU–Dortmund/CN=YYYYYY YYYYYY" kg0081
3 "/C=DE/O=GermanGrid/OU=TU–Dortmund/CN=ZZZZZZ ZZZZZZ" hp0007
```

Um den Mitgliedern einer virtuellen Organisation die Nutzung eine Compute Cloud Ressource über OpenNebula zu ermöglichen, benötigt man einen Mechanismus, der die initial leere Nutzerverwaltung mit Inhalt füllt und periodisch aktualisiert. Hierzu bietet sich das `dgridmap`-Skript[13] an, welches bereits die Grid Middlewares gLite, Globus Toolkit und UNICORE unterstützt und entsprechend erweitert werden kann.

Für D-Grid Nutzer ist die zuvor beschriebene Verwendung von *access* und *secret key* umständlich, weshalb die Erweiterung von OpenNebula um eine X.509 Unterstützung wünschenswert ist. Das nächste größere OpenNebula Release 1.6 soll bereits verschiedene Autorisations– und Authentifikationsmechanismen für Nutzer enthalten. Hierunter fällt auch die Interaktion mit LDAP-, PAM- und X.509-basierten Autorisationsbackends. Geplant ist die Möglichkeit zur Authentifikation mittels eines kurzlebigen Proxy (Stellvertreter-Zertifikats), welcher durch Grid-Mechanismen wie `grid-proxy-init` oder `voms-proxy -init` erzeugt wurde. Dies erleichtert D-Grid den Zugang zu Compute Cloud Ressourcen.

Weitere offene Punkte in Zusammenhang mit der Nutzerverwaltung sind die Umsetzung der Attribut-basierten Autorisation und damit einhergehend ii) die Abbildung der Strukturen virtueller Organisationen auf Clouds.

5.2 Informationssystem

Jede im D-Grid angebotene Grid Middleware besitzt ein eigenes Informationssystem. Bei gLite besteht es aus Site- und TopBDII, bei Globus Toolkit aus dem (Web-) MDS und bei UNICORE6 aus dem CIS (Common Information Service).
Das D-Grid Gap Projekt D-MON [14], entwickelte ein übergeordnetes Informationssystem, welches die Informationen aus den Middleware-spezifischen Systemen zusammenführt und einheitlich präsentiert. Abbildung 4 zeigt die Architektur der D-MON Software. Die Abfrage der einzelnen Informationssysteme erfolgt über Adapter, die die erhaltenen Daten in ein unabhängiges Datenformat konvertieren.
Zur Bereitstellung und Integration von Informationen aus der Cloud Middleware in D-MON ist die Entwicklung eines weiteren Adapters notwendig. Zudem sind relevante Informationen der Cloud Middleware zu spezifizieren, welche über diesen Adapter publiziert werden. Diese Größen können die verwendete Virtualisierungstechnologie (z. B. Xen, VMware) ebenso enthalten wie verfügbare Templates und Limits hinsichtlich max. Core-Anzahl und Hauptspeicher pro virtueller Appliance.

[13] http://www.d-grid.de/index.php?id=335
[14] http://www.d-grid.de/index.php?id=401

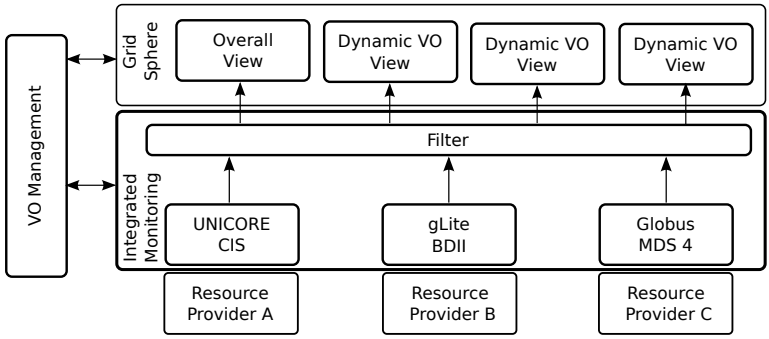


Abbildung 4: Vereinfachte D-MON Architektur

5.3 Accounting

Bisher sind alle Jobs über Schnittstellen der Grid Middleware in das LRMS (vgl. Abbildung 2) eingereicht worden. Durch die Einführung einer Compute Cloud Schnittstelle ändert sich dies. Jobs, in diesem Fall virtuelle Appliances, starten nicht auf LRMS sondern auf Fabric Ebene.
Für ein Grid-umfassendes Accounting für virtuelle Organisationen zu ermöglichen, wird im D-Grid das OGF-UR (Open Grid Forum – Usage Record) Format [Can06] verwendet. Ein Dienst auf der Ressource generiert aus Informationen der LRMS Ebene jobspezifische Accountingdaten und publiziert diese als UR (vgl. Listing 2 für ein Beispiel) an einen zentralen Dienst des D-Grid.

Listing 2: Beispiel eines Usage Records

```
1 JOB_TYPE=local
2 GlueHostBenchmarkSI00=43.7
3 GlueHostBenchmarkSF00=36.1
4 ACCTLOG:11/01/2009 17:30:39;E;376020.udo-torque01.grid.tu-
      dortmund.de;user=opssgm group=ops jobname=STDIN queue=
      ops ctime=1257092411 qtime=1
5 257092411 etime=1257092411 start=1257092412 exec_host=udo-
      wn034.grid.tu-dortmund.de/0 Resource_List.cput=48:00:00
      Resource_List.neednodes=1
6 Resource_List.nodect=1 Resource_List.nodes=1 Resource_List.
      walltime=72:00:00 session=9426 end=1257093039
      Exit_status=0 resources_used.cput=0
7 0:00:56 resources_used.mem=51508kb resources_used.vmem
      =150428kb resources_used.walltime=00:10:27
```

Für das am DGRZR verwendete OpenNebula fehlt ein solches Accounting-Werkzeug. Wie in Abschnitt 5.1 dargelegt, nutzt es zur Speicherung persistenter Informationen eine SQLite3 Datenbank. Über den Zugriff auf u. a. die *history* Tabelle (vgl. Tabelle 1) können

zu erstellende Implementierungen des Accounting-Werkzeugs auf die notwendigen Daten zur Generierung eines Accounting-Eintrags zugreifen. Die *vm_attributes* Tabelle (vgl. Ta-

vid	host_name	stime	etime	pstime	petime
13	udo-bl2313	1258384216	1258384219	1258384216	1258384219
12	udo-bl1107	1258384210	1258384247	1258384210	1258384244

Tabelle 1: Auszug der history Tabelle in der one.db

belle 2) stellt eine der weiteren zu inspizierenden Tabellen dar. Sie enthält Informationen über die von der Appliance angeforderten Ressourcen, währen die *history* Tabelle Start- und Stopp-Zeitpunkte festhält.

id	name	type	value
12	CPU	0	0.5
12	MEMORY	0	256
12	NAME	0	centos.5-3.x86
12	VMID	0	12

Tabelle 2: Auszug der vm_attribute Tabelle in der one.db

Insgesamt wird die Entsprechung der Usage Records für verbrauchte Cloud Ressourcen mit dem vom OGF vorgeschlagenen Format angestrebt. Dadurch können diese Records vom zentralen D-Grid Accounting Dienst verarbeitet werden.

5.4 Zusammenspiel von Grid Batchsystem und OpenNebula am DGRZR

Am DGRZR besteht das Batchsystem auf LRMS Ebene aus einer Kombination von Torque und MAUI. Letzteres dient als Scheduler. Über die Grid Schnittstellen eingereichte Jobs werden vom Scheduler an Workernodes weitergeleitet.
OpenNebula verwendet einen internen Scheduler für die Zuweisung von virtuellen Appliances zu physischen Rechnern. Das dabei verwendete Verfahren unterstützt die Rank Scheduling Policy, welche Ressourcen priorisiert, die gut auf die Anforderungen der Appliance passen. Der Scheduler ist als separater Prozess entworfen und somit austauschbar. Eine Unterstützung einer Advance Reservation von Kapazitäten, wie man sie von LRMS kennt, ist durch die Integration von Haizea [15] als Scheduler möglich.

Eine mögliche Form der Kooperation beider Komponenten besteht im dynamischen Deployment von job-spezifischen Workernodes [Kon09]. In dieser Arbeit wird Annahme getroffen, dass die Anzahl an unterschiedlichen Job-Typen in einem Batchsystem limitiert ist. Auf Basis der Job-Typen werden Queues im Batchsystem generiert – ein Job-Typ entspricht genau einer Queue – und deren Füllstände periodisch überwacht. Zudem ist jeder Queue zu Beginn eine Menge von Workernodes zugeordnet.

[15] http://haizea.cs.uchicago.edu/

Sofern in einer der Queues keine Jobs vorliegen und in einer anderen nicht alle Jobs sofort gestartet werden können, greift eine übergeordnete Instanz ein. Diese Instanz fährt einige Workernodes, die der leeren Queue zugeordnet sind, herunter. Anschließend starten auf den freigewordenen physischen Ressourcen Workernodes, die dem Job-Typ der überfüllten Queue genügen. Nachdem die Workernodes sich beim Batchsystem Server angemeldet haben, beginnen sie mit der Jobabarbeitung aus der überfüllten Queue.

Sofern das Batchsystem nicht vollständig ausgelastet ist, können nicht benötigte Workernodes (Virtual Appliances) ebenso herunter gefahren und zugehörige physische Knoten in einen Standby-Modus versetzt werden. Unter dem Aspekt von Green-IT ist dies eine sinnvolle Maßnahme.

6 Zusammenfassung

Cloud Computing etablierte sich in kurzer Zeit zu einer neuen enabling technology im IT Sektor. Ein wesentlicher Grund hierfür liegt in dem hohen Maß an Flexibilität, welches sowohl Ressourcenbetreiber als auch Anwender gewinnen. Ersteren ermöglicht Cloud Computing eine gesteigerte Ressourcenauslastung und letzteren einen einfacheren Zugang zu Ressourcen als es mit dem Grid Computing derzeit möglich ist.

In diesem Kontext wurde die Erweiterung einer D-Grid Ressource um eine Compute Cloud Schnittstelle untersucht. Die Installation von OpenNebula am D-Grid Ressourcen Zentrum Ruhr sowie weitere Maßnahmen ermöglichen insgesamt die Einreichung von Jobs (Virtual Appliances) über die Cloud Middleware. Weiterführend wurde die Frage nach notwendigen Arbeiten zur Integration der Compute Cloud Middleware in das D-Grid beantwortet. Für die identifizierten offenen Punkte wurden Lösungsansätze andiskutiert, die in Folgearbeiten ausgebaut werden.

Literatur

[Buy09] Cloudbus Toolkit for Market-Oriented Cloud Computing, R. Buyya, S. Pandey und C. Vecchiola, Lecture Notes in Computer Science, Vol. 5931, Seiten 24–44, 2009.

[Can06] Aggregate Usage Representation Recommendation (Version 1.0), P. Canal, J. Gordon, D. Kant, A. Khan, R. M. Piro, X. Chen, Open Grid Forum, 2006.

[Edm09] Open Cloud Computing Interface Specification Version 5, A. Edmonds, S. Johnston, G. Mazzaferro, T. Metsch und A. Merzky, Open Grid Forum, http://forge.ogf.org/sf/go/doc15731 September 2009.

[Fos01] The Anatomy of the Grid: Enabling Scalable Virtual Organizations, I. Foster, C. Kesselman und S. Tuecke, International Journal of Supercomputer Applications, Vol. 15, 2001.

[Kon09] Dynamisches Management virtueller Maschinen auf den High-Performance Computing Ressourcen der Technischen Universität Dortmund, B. N. Konrad, Diplomarbeit, 2009.

[Llo09] Dynamic Provisioning of Virtual Clusters for Grid Computing, M. Rodríguez, D. Tapiador, J. Fontán, E. Huedo, R. S. Montero und I. M. Llorente, Proceedings Euro-Par 2008 Workshops - Parallel Processing: VHPC 2008, UNICORE 2008, HPPC 2008, SGS 2008, PROPER 2008, ROIA 2008, and DPA 2008, Las Palmas de Gran Canaria, Spain, August 25-26, 2008, Revised Selected Papers, Seiten 23–32, 2009.

[Roc09] The RESERVOIR Model and Architecture for Open Federated Cloud Computing, B. Rochwerger, J. Caceres, R.S. Montero,D. Breitgand,E. Elmroth,A. Galis,E. Levy, I.M. Llorente,K. Nagin,Y. Wolfsthal, IBM Systems Journal, Vol. 53, No. 4, 2009.

[Sot09] Virtual Infrastructure Management in Private and Hybrid Clouds B. Sotomayor, R. S. Montero, I. M. Llorente und I. Foster, IEEE Internet Computing, Vol. 13, No. 5, October 2009

[Vaq09] A break in the clouds: towards a cloud definition, L. M. Vaquero, L. Rodero-Merino, J. Caceres und M. Lindner, ACM SIGCOMM Computer Communication Review, Volume 39, No. 1, Seiten 50–55, 2009.

CollaboCloud - Kollaborationsplattform in der Cloud

Christoph Reich, Hendrik Kuijs und David Schröpfer
Informatik und Rechenzentrum der
Hochschule Furtwangen University, Deutschland
{christoph.reich, hendrik.kuijs, david.schroepfer}@hs-furtwangen.de

Abstract: Cloud Computing ermöglicht es, Software "on-demand" über das Internet zu liefern. Dieses Dokument zeigt wie die Plattform CollaboCloud aufgebaut ist und als SaaS in einer Cloud der Hochschule Furtwangen gehostet wird. CollaboCloud kommt an der Hochschule Furtwangen in den Bereichen Projektzusammenarbeit und Forschungskollaboration zum Einsatz. Besonders interessant sind die Möglichkeiten der Bildung von Föderationen mit Shibboleth, die Skalierbarkeit der Plattform durch Clustering und die automatische bedarfsorientierte Verlagerung der Plattform von der hochschuleigenen "private" Cloud, CloudIA – Cloud Infrastructure and Application – in die "public" Cloud von Amazon.

1 Einführung

Cloud Computing liefert Infrastruktur- und Software-as-a-Service (IaaS und SaaS) auf einem einfachen "Pay-per-use" Geschäftsmodell. Dies ermöglicht kleineren und mittleren Unternehmen (KMU) Hardware-Ressourcen zu sparen, indem bei Bedarf Spitzenlasten in die Cloud ausgelagert werden. Die Hochschule Furtwangen University (HFU) arbeitet an der Erstellung einer "private" Cloud, die IaaS und SaaS für die Lehre und die Forschung zur Verfügung stellt. Eines der ersten Projekte hierbei war CollaboCloud, eine SaaS für E-Learning, Projektzusammenarbeit und Kollaborationswerkzeug zur Unterstützung der Lehre und der Forschung. Das "on-demand"-Instanziieren der Software wird an der HFU genutzt, um Firmen eine Weiterbildungsplattform zur Verfügung zu stellen, um die Kollaboration zwischen Hochschulangehörigen und der Industrie oder die Zusammenarbeit der Studierenden untereinander in kleinen abgeschlossenen Projekten zu unterstützten. Von Anfang an war wichtig, eine automatische Lastverteilung zu realisieren, die bei knappen Ressourcen an der Hochschule die SaaS Applikation in eine "public" Cloud wie Amazon auslagert.

Das Dokument ist wie folgt organisiert: Kapitel 2 diskutiert verwandte Arbeiten. Kapitel 3 erklärt die Infrastruktur CloudIA, in der das Kollaborationswerkzeug als SaaS läuft. Kapitel 4 stellt Details zu CollaboCloud als SaaS, Skalierbarkeit, unterschiedliche Authentifzierungsmöglichkeiten, sowie die Erweiterung von SVN um Shibboleth vor. Kapitel 5 zeigt Erfahrungen beim Bau und Betrieb von CollaboCloud und abschließend wird im Kapitel 6 ein Fazit gezogen.

2 Verwandte Arbeiten

Es gibt eine umfangreiche Auswahl an web-basierten Kollaborationswerkzeugen (siehe [Wik]). Jedoch haben viele das Problem der horizontalen Skalierung, welches bei CollaboCloud durch Clustering gelöst wird. Ein weiteres Problem einiger Tools ist die Möglichkeit der einfachen Integration der Authentifizierung mit Single-Sign-On in eine bestehende Infrastruktur. Marktführer ist hier das Produkt von Microsoft: Office SharePoint Server 2007 [Sha]. Dieses integriert sich hervorragend in die Microsoft Welt (Active Directory, etc.), ist jedoch für die Hochschulwelt, die oft auf einer Unix-Umgebung aufbaut, ungeeignet.

BlueSky Cloud [DZQ+09] weist virtuelle Maschinen mit E-Learning-Systemen auf Nachfrage zu. Darüber hinaus verbindet BlueSky traditionelle Middleware-Funktionen (z. B. Load-Balancing und Daten-Caching) für E-Learning-Systeme. CollaboCloud kann auch als E-Learning Plattform verwendet werden und hat seine Stärken besonders in der Unterstützung der Kollaboration.

Der semantische Informationsmediator, Collaboration Cloud [col], greift auf verteilt vorliegende heterogene Datenbestände zu, um die Daten zu analysieren und hat nur vom Namen her Gemeinsamkeiten mit CollaboCloud. Die Collaboration Cloud verarbeitet Daten unterschiedlichster Quellen und verknüpft diese semantisch und hat nichts mit Kollaboration von Personen zu tun.

LotusLive Connections [Lot] ist ein Produkt von IBM, das als SaaS zur Verfügung gestellt wird. Dessen Funktionalität umfasst Social Networking, gemeinsame Datennutzung, Instant Messaging und Aktivitätenverwaltung. CollaboCloud dagegen hat zusätzliche Funktionalitäten wie Foren und Versionsmanagement und ist Freeware.

Die interaktive Anwendung chatter [cha] von salesforce.com bietet ein soziales Netzwerk das hilft sich einen Überblick über Abläufe und Ereignisse von Mitarbeitern, Gruppen, Dokumenten und Anwendungsdaten zu verschaffen. Das Ablegen von Dateien oder das gemeinsame Schreiben von Dokumenten im Wiki steht hingegen nur dem Benutzer in der CollaboCloud zur Verfügung.

3 Cloud Infrastructure and Application (CloudIA)

CloudIA, Cloud Infrastructure and Application, ist eine marktorientierte Cloud Plattform, die verschiedene Virtualisierungstechnologien vereint und den interessierten Hochschulpartnern (z.B. Industrie, Institute, etc.) und Studierenden als Infrastruktur zur Zusammenarbeit dienen soll. Die CloudIA Plattform erweitert die Open Source Cloud Plattform OpenNebula [Ope] um neue Funktionalitäten, wie z.B. eine Kapazitätsplanung, Single-Sign-On (SSO) mit Shibboleth [Shi] und ein zusätzliches QoS-Monitoring. CloudIA nutzt die verschiedenen Virtualisierungstechnologien, wie Xen [BDF+03], KVM [Qum] und VMware [VMw], bietet QoS Überwachung, Sicherheit, etc. wie in der Übersicht von Abbildung 1 dargestellt. Das Cloud Management System (CLMS) (Abb. 1) ist in mehrere Schichten, wie *User Interface*, *Business*, *System*, and *Resource Interface*, aufgeteilt, um

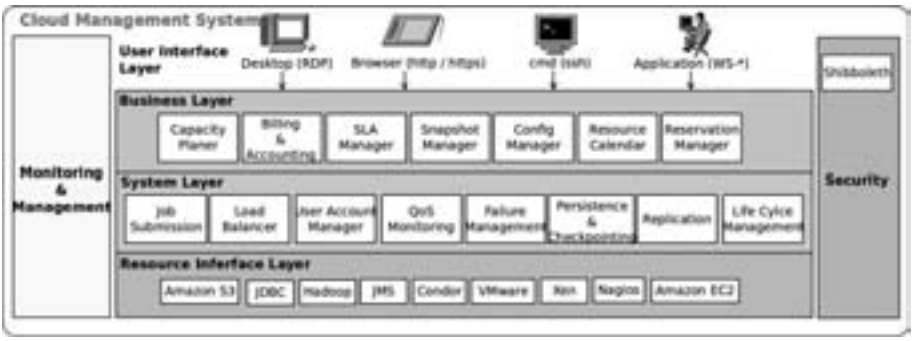


Abbildung 1: Cloud Management System of CloudIA.

das System in einem hohen Maße wartbar und erweiterbar zu halten. Besonders *Monitoring & Management* und *Security* spannt sich über alle Schichten hinweg, um die hohe Verfügbarkeit und Sicherheit der einzelnen Komponenten zu gewährleisten. Nachfolgend werden die einzelnen Schichten kurz erklärt:

User Interface Layer stellt verschiedene Access Points zur Verfügung, um einen Benutzer- und/oder Administrator-Zugriff auf das Cloud System zu ermöglichen.

Business Layer verwaltet die vertraglichen Vereinbarungen (Service Level Agreements: SLAs) zwischen Anbieter und Nutzer und überwacht deren QoS. Darüber hinaus können Nutzer VMs im Voraus reservieren und ihre persönlichen VMs verwalten.

System Layer ist für den täglichen Betrieb des CLMS zuständig, wie z.B. Übergeben von Jobs, die Verwaltung von Benutzerkonten und QoS-Monitoring.

Resource Interface Layer befasst sich mit der physischen Hardware und beherbergt diverse Schnittstellen und Plugins für verschiedene Virtualisierungslösungen, Datenbanken, verteilte Systeme und andere Technologien, wie Überwachung mit Nagios [Nag].

Monitoring & Management Component wird benötigt, um die Zuverlässigkeit der einzelnen Schichten im Cloud-Management-System zu gewährleisten. System-Administratoren können mit dieser Komponente Aktivitäten in den einzelnen Schichten initiieren, sodass im Falle von Fehlern, SLA-Zielkonflikten etc. mit Hilfe des Loggings Reports erstellt werden können.

Security Component gewährleistet die Privatsphäre, Wiederherstellung, Integrität und Sicherheit der Benutzer-Daten und -Transaktionen. Neben den technischen Lösungen sind auch Themen in Bereichen wie Einhaltung gesetzlicher Vorschriften und Data Auditing sehr wichtig. Hier findet sich ebenfalls das Shibboleth-Modul, das im nächsten Kapitel 4.3 näher diskutiert wird.

4 CollaboCloud: Kollaboration als SaaS

Die Hochschule nutzt die Open Source "Online Learning and Training" (OLAT) Plattform [OLA] als Basissystem für die Kollaborationsplattform CollaboCloud. Die Stärken von OLAT sind vor allem der einfache Umgang mit Arbeitsgruppen. Jeder OLAT-Nutzer kann eigene Arbeitsgruppen anlegen und selbst verwalten. Z.B. andere zur Arbeitsgruppe einladen und den Funktionsumfang einer Arbeitsgruppe (Kalender, Forum, Wiki, Benachrichtigung, Chat und Info-Seite) festlegen. Diese Flexibilität ist herausragend und wird aus unserer Erfahrung an der HFU sehr gut angenommen. Ergänzt wird das System durch das Versionierungssystem Subversion [svn], welches um Shibboleth-Funktionalitäten erweitert und mit der OLAT-Plattform verknüpft wurde (siehe Kapitel 4.4). Die CollaboCloud-Plattform wird an der HFU für unterschiedlichste Anwendungsfälle genutzt:

- als HFU-interne Projektmanagement-Plattform, die dabei vor allem die Komponente: Projektverwaltung der OLAT-Plattform nutzt und
- als Kollaborationswerkzeug für die Zusammenarbeit von Hochschulangehörigen, Industrie- und Forschungspartnern.

Ziel war es die OLAT-Plattform als SaaS zur Verfügung zu stellen. Dazu sollen die fünf wichtigsten charakteristischen Eigenschaften einer "Software as a Service" (SaaS) erfüllt sein:

1. **Zugriff über das Internet:** Da OLAT eine web-basierende Software ist und eine Browser-basierte Nutzung vorsieht, kann weltweit über das Internet mit jedem Gerät, das mit einem Browser ausgerüstet ist, darauf zugegriffen werden.
2. **Software "on demand":** Nachdem der Nutzer mit Hilfe des speziell entwickelten Management-User-Interface seine OLAT-Instanz konfiguriert hat (Layout, Accounts, bestehende Daten eingespielt, etc.) kann die Instanz bedarfsgerechte gestartet und gestoppt werden.
3. **Skalierung von SaaS:** Im Kapitel 4.1 wird dieses Thema ausführlich diskutiert.
4. **Überwachung von SaaS:** Die CloudIA-Plattform erlaubt die Überwachung von SaaS Services. Darüber hinaus können die CollaboCloud-Services in eine bestehende Nagios Infrastruktur [Nag] integriert werden.
5. **Ortsunabhängigkeit von SaaS:** Falls die Skalierung in der lokalen "private" Cloud CloudIA nicht mehr ausreicht, kann jederzeit die CollaboCloud-Instanz bei Amazon gehostet werden. Für den Nutzer ist dies völlig transparent (siehe Kapitel 4.2).

4.1 Aufbau von CollaboCloud

CollaboCloud besteht prinzipiell aus einer OLAT-Plattform, einem Instant-Messaging Server und einem Subversion-Service (siehe Abbildung 2). OLAT ist eine Java-Web-Applikation, die aus den Komponenten Apache Tomcat, MySQL und Apache HTTP-Server

besteht. Das Kernsystem OLAT 6.x basiert auf einer klassische Multi-Tier Architektur (Client-, Präsentation-, Business-, Integration- und Resource-Tier), wie in den Core J2EE-Pattern [AMC01] beschrieben. Dessen Komponenten, wie z.B. Lern-, Blackboard- oder Nachrichten-Module, werden im Apache Tomcat gehostet. Eine detaillierte Architekturbeschreibung findet man im Dokument: "Architektur eines webbasierten Lernsystems" [Gna01]. CollaboCloud bietet auch direkte Monitoring-Funktionalitäten über MRTG [Oet] an, um Systemparameter zu protokollieren und grafisch Darzustellen. Diese Elemente werden in der kleinsten Ausbaustufe zusammen auf einem System installiert.

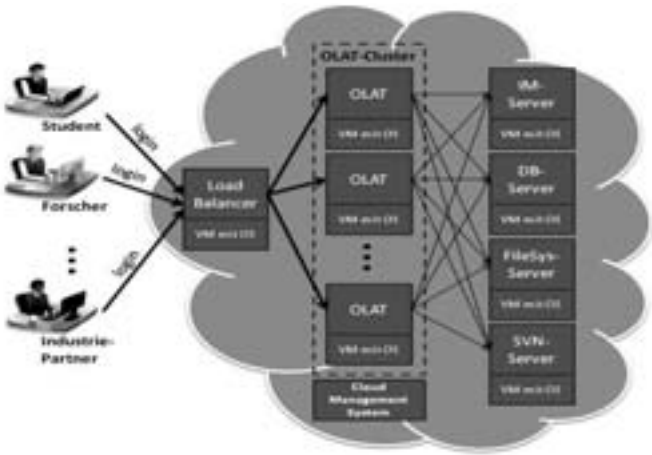


Abbildung 2: CollaboCloud Cluster

Für die Skalierbarkeit der Plattform wird OLAT als Cluster konfiguriert, was eine dynamische Lastanpassung der wichtigsten Komponenten ermöglicht. Die Abbildung 2 zeigt den kompletten Aufbau eines OLAT-Clusters. Der Loadbalancer verteilt die Anfragen gleichmäßig auf die OLAT-Instanzen, welche die Services Filesystem, Datenbank und Instant Messenger gemeinsam nutzen.

4.2 CollaboCloud "On Demand"

Normalerweise wird die CollaboCloud in der "private" Cloud CloudIA gehostet. Kommt es jedoch zu Ressourcen-Engpässen ermöglicht das Cloud Management Module (siehe Abbildung 3) die CollaboCloud auch in Amazon zu hosten. Dies geschieht völlig automatisch und transparent für den Nutzer. Das Cloud Management Module weist bei Überlast der "private cloud" automatisch eine Instanz in Amazon zu und kontrolliert die Zuordnung der Nutzer zu den Instanzen in der Amazon Cloud.

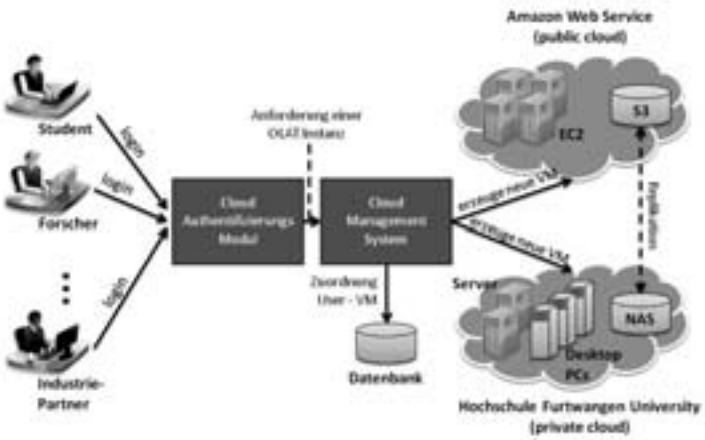


Abbildung 3: Übersicht der CollaboCloud on Demand Infrastruktur

4.3 Authentifizierungsarten: lokal, LDAP, Shibboleth

Einzigartig macht die CollaboCloud die Möglichkeit Shibboleth [Shi] als Authentifizierung und Autorisierung einzusetzen. Das Konzept von Shibboleth sieht vor, dass der Benutzer sich nur einmal beim Identity Provider seiner Heimatorganisation authentisieren muss, um ortsunabhängig auf Dienste oder lizenzierte Inhalte verschiedener Anbieter zugreifen zu können (Single-Sign-On). Dazu müssen die Services Shibboleth-fähig sein, was OLAT nativ zur Verfügung stellt und für Subversion durch eine Eigenentwicklung der HFU erreicht wird (siehe Kapitel 4.4).

Die CollaboCloud-Plattform ermöglicht insgesamt 3 Arten von User-Management:

Direkt-Administration ist für kleine User-Mengen geeignet. Der OLAT-Administrator nutzt die OLAT-Admin Oberfläche um einzelne Accounts anzulegen oder zu löschen.

LDAP Lightweight Directory Access Protocol [lda08] ist ein sehr verbreiteter Verzeichnisdienst zur Datenhaltung von Identitäten. Durch die Konfiguration zu Beginn einer neuen OLAT-Instanz kann auch ein bestehender LDAP-Server einer Organisation zur Authentifizierung der OLAT-User angegeben werden.

Shibboleth ist ein föderativer Ansatz. Falls eine Institution schon einer Föderation, wie z.B. DFN-AAI beigetreten ist, kann mit geringen Konfigurationsänderungen an der OLAT-Instanz auch anderen Föderations-Mitgliedern Zugriff gewährt werden. Die Einhaltung der gemeinsamen Regeln und Standards wird durch die Mitgliedschaft einer Föderation gewährleistet. Die Authentifizierung und die Zugriffe auf die jeweiligen Service Provider erfolgen beim Identity Provider (IdP) der jeweiligen Heimatorganisation.

4.4 SVN als Erweiterung der CollaboCloud

Das Versionierungssystem Subversion wird in der CollaboCloud für die gemeinsame Arbeit mehrerer Nutzer an einem Projekt verwendet. Da es mit Shibboleth nicht möglich ist, für alle Anwender einen Systemaccount auf der SVN-Instanz vorzuhalten, wurden umfangreiche Anpassungen an der Standard-SVN-Installation vorgenommen.

Um allen Nutzern innerhalb der Cloud automatisch einen Zugriff auf das Versionierungssystem zu gewähren, musste eine Verwaltungsoberfläche entwickelt werden, welche über einen Browser erreicht werden kann. Hierzu wird neben SVN der HTTP-Server Apache mit den Modulen dav_svn, ldap und shib verwendet. Mittels der Authentifizierung über Shibboleth wird der Zugriff auf die Verwaltungsoberfläche gewährt. Jeder Nutzer kann über diese GUI beliebig viele Repositories erstellen und verwalten. Durch die Kopplung an den zentralen LDAP Verzeichnisserver können weitere Anwender als zugriffsberechtigte Nutzer zu einem Repository hinzugefügt werden. Die Umsetzung der vergebenen Rechte für Anwender (Lesen, Schreiben, Verwaltung) übernimmt Apache als zentrale Komponente des Systems. Die gesamte Konfiguration aller auf der Instanz vorhandenen Projekte wird in mehreren Apache-Konfigurationsdateien verwaltet. Bei jedem Zugriff auf die Verwaltungsoberfläche wird geprüft, zu welchen Repositories der Nutzer Zugriffsrechte besitzt und wie hoch diese sind.

Durch die vorgestellte Gesamtstruktur wird erreicht, dass für die Nutzung des SVN-Service kein zusätzlicher administrativer Aufwand entsteht. Alle Nutzer, die innerhalb der CollaboCloud über den Shibboleth-IdP authentifiziert werden, erhalten automatisch Zugriff auf den Dienst. Die flexible, individuelle Verwaltung von Repositories über die Weboberfläche bietet einen, im Gegensatz zu bisher verfügbaren Lösungen, hohen Komfort für Anwender.

5 Gesammelte Erfahrungen

Typische Virtualisierungs-Szenarien sind das Erstellen einfacher VMs und der Einsatz von vorinstallierten VM Images. Eine Basisinstanz kann jedoch nicht mehrfach, je nach Bedarf, ohne entsprechende Anpassungen instantiiert werden. Zuerst muss eine Personalisierung der Images erfolgen. Hierzu zählen die Vergabe von IP-Adressen, die Installation von Zertifikaten, das Setzen von Admin-Passwörtern, das Einrichten von Nutzern, die Anpassung von GUI-Styles etc. Dies erfordert aus administrativer Sicht viel Vorarbeit. Die Personalisierung der Images teilt sich in technische Vorbedingungen um die spätere Instanz für die Nutzer zugänglich zu machen (DNS, Zertifikat, Anbindung an SSO), sowie in administrative Vorbedingungen, um die laufende Instanz durch einen Administrator verwalten und anpassen zu können. Für diese initialen Anpassungen wird ein User-Interface eingesetzt, das den Administrator der Instanz durch die benötigten Schritte führt. Dieses wird zwischen dem Starten der Instanz und dem Starten der Dienste ausgeführt und legt sowohl die technischen, als auch die administrativen Grundsteine. Abschließend folgt eine Gegenüberstellung der Request-Response-Zeit der VM in Amazon EC2 und CloudIA.

5.1 Technische Vorbedingungen für CollaboCloud

Eine Anforderung für die Nutzung einer Kollaborationsplattform wie der CollaboCloud ist die Gewährleistung der Sicherheit des Datenaustauschs zwischen Client (Browser) und Server. Dies kann durch eine SSL-Verschlüsselung erreicht werden. Die Erstellung der entsprechenden Zertifikate widerspricht jedoch dem Anspruch, flexibel und schnell Instanzen der CollaboCloud starten und stoppen zu können. Da gültige, nicht selbst signierte Zertifikate zumindest an DNS-Namen gekoppelt sind, kann durch ein Vorhalten eines Pools von DNS-Einträgen und den jeweiligen vorgefertigten Zertifikaten der Startprozess einer Instanz um den Beantragungszeitraum verkürzt werden. Dennoch muss nach dem Starten einer Instanz der DNS-Administrator die IP der Instanz mit dem jeweiligen DNS-Eintrag verknüpfen. Danach wird das Zertifikat in die Konfiguration des Apache HTTP-Servers, sowie, bei Verwendung als SSO-Dienst mit Shibboleth, in die entsprechenden Konfigurationsdateien von Shibboleth eingetragen. Wird die CollaboCloud ohne Shibboleth und damit verbunden ohne den Subversion-Dienst verwendet, muss Anstelle von Shibboleth entweder eine LDAP-Verbindung konfiguriert werden (dies geschieht über die OLAT-Initial-Konfiguration), oder die Konfiguration einer externen Nutzerverwaltung entfällt ganz. In diesem Fall werden die Nutzer nach dem Start von OLAT lokal eingepflegt und in der lokalen Datenbank verwaltet.

5.2 Administrative Vorbedingungen für CollaboCloud

Um die laufende Instanz zu verwalten sind initiale Zugangsdaten für den Administrator-Account von OLAT erforderlich. OLAT selbst ermöglicht anschließend die Anpassung der Plattform zur Laufzeit. So können lokal Nutzerrechte vergeben werden, Quotas für den Up- und Download von Daten angepasst und Sprachanpassungen vorgenommen werden.

5.3 Performance in CloudIA gegenüber Amazon EC2

Im folgenden Experiment (vgl. [DSR+10]) werden die Request-/Response-Zeiten von einer CollaboCloud-Installation in der “private Cloud” (CloudIA) mit einer Installation in der “public Cloud” (Amazon EC2) verglichen.

	CloudIA	Amazon EC2	
	Instanz	large	extra large
Prozessoren	8	2	4
CPU Typ (Intel(R) Xeon(R))	E5504	E5430	E5430
CPU Takt	2.00GHz	2.66GHz	2.66GHz
gesamt Arb. Speicher (kB)	12330508	7872040	15736360

Tabelle 1: Hardware-Konfiguration für das CollaboCloud Experiment.

Für das Experiment wird ein Host in CloudIA und jeweils eine “large” und eine “extra

large” Instanz in der Public Cloud von Amazon verwendet. Tabelle 1 zeigt die jeweiligen Hardware-Konfigurationen der Instanzen.

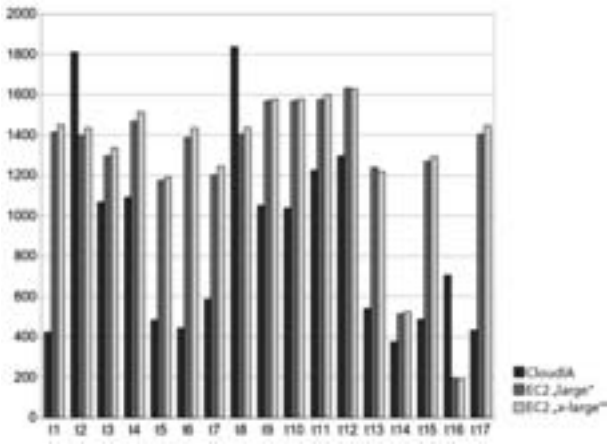


Abbildung 4: Request-Response-Zeit (ms)

Testfall	Beschreibung
t1	Startseite (dmz)
t2	Login
t3	Seite “Home”
t4	Seite “Kalender”
t5	Seite “Katalog”
t6	Suche nach Dokument
t7	Suche nach Demo-Kurs
t8	Öffne Demo-Kurs
t9	Seite “Self-HTML” im Demo-Kurs
t10	Seite “Forum” im Demo-Kurs
t11	Seite “Content-Package” im Demo-Kurs
t12	Seite “Datei-Diskussion” im Demo-Kurs
t13	Download 4MByte Datei
t14	Download 1MByte Datei
t15	Öffne Suche
t16	Logout
t17	Startseite (dmz)

Abbildung 5: JMeter Testplan

Auf den einzelnen Hosts wird die selbe Software-Konfiguration verwendet. Die Lasttests werden mit Apache JMeter [jme] durchgeführt.Mit dem JMeter-Testplan (vgl. Abbildung 5) werden 200 Nutzer zeitgleich simuliert. In Abbildung 4 sind die gemittelten Request-Response-Zeiten der einzelnen Instanzen dargestellt. Mit der Ausnahme von t2 (Login) und t8 (Öffne Demo-Kurs) sind die Zeiten in CloudIA geringer als in den Amazon Instanzen. Die Antworten der Instanzen in Amazon sind jedoch ebenfalls gut und stellen keine Beeinträchtigung für deren Nutzung dar.

6 Zusammenfassung und Ausblick

Dieser Artikel beschreibt das Kollaborationswerkzeug CollaboCloud, welches auf der HFU Cloud-Plattform CloudIA basiert. Diskutiert wurden die wichtigen Charaktereigenschaften einer SaaS Anwendung, wie beispielsweise “on-demand”. Besonders die bedarfsorientierte Auslagerung in die “public” Cloud Amazon und die Authentifizierung durch Shibboleth machen die CollaboCloud Applikation einzigartig. Die dazu entstandene Erweiterung des Subversion-Dienstes durch Shibboleth wurde im Kapitel 4.4 dargelegt. In Kapitel 5.1 wurde vor allem auf die Erfahrungen zur benötigten Zertifikatsverwaltung eingegangen. Zukünftig wird noch daran gearbeitet ein Web-Meeting System, wie Dimdim [dim], zu integrieren.

Literatur

[AMC01] Deepak Alur, Dan Malks und John Crupi. *Core J2EE Patterns: Best Practices and Design Strategies*. Prentice Hall PTR, Upper Saddle River, NJ, USA, 2001.

[BDF+03] P. Barham, B. Dragovic, K. Fraser, S. Hand, T. Harris, A. Ho, R. Neugebauer, I. Pratt und A. Warfield. Xen and The Art of Virtualization. In *Proceedings of the 19th ACM Symposium on Operating Systems Principles (SOSP'03)*, New York, USA, Oct. 19–22 2003.

[cha] Chatter from Salesforce. http://www.salesforce.com/de/chatter/.

[col] CollabCloud - Collaboration Cloud. http://www.collaborationcloud.de/Home/.

[dim] dimdim - Web Meeting Software. http://www.dimdim.com/.

[DSR+10] Frank Doelitzscher, Anthony Sulistio, Christoph Reich, Hendrik Kuijs und David Wolf. Private Cloud for Collaboration and e-Learning Services: from IaaS to SaaS. Technical Report CRL-2010-01, Hochschule Furtwangen University, Feb. 2010.

[DZQ+09] Bo Dong, Qinghua Zheng, Mu Qiao, Jian Shu und Jie Yang. BlueSky Cloud Framework: An E-Learning Framework Embracing Cloud Computing. In Martin Gilje Jaatun, Gansen Zhao und Chunming Rong, Herausgeber, *CloudCom*, volume 5931 of *Lecture Notes in Computer Science*, pages 577–582. Springer, 2009.

[Gna01] Florian Gnaegi. Architektur eines webbasierten Lernsystems. Master's thesis, Institut für Informatik der Universität Zürich, 2001.

[jme] Apache JMeter. http://jakarta.apache.org/jmeter/.

[lda08] RFC4510: Lightweight Directory Access Protocol (LDAP). http://tools.ietf.org/html/rfc4510, june 2008.

[Lot] Lotuslive Connection from IBM. https://www.lotuslive.com/de/services/connections.

[Nag] Nagios. IT Infrastructure Monitoring. http://www.nagios.org/.

[Oet] Tobi Oetiker. Tobi Oetiker's MRTG - The Multi Router Traffic Grapher. http://oss.oetiker.ch/mrtg/.

[OLA] OLAT. Online Learning And Training (OLAT). http://www.olat.org/.

[Ope] OpenNebula. OpenNebula: The Open Source Toolkit for Cloud Computing. http://www.opennebula.org/.

[Qum] Qumranet. KVM: White Paper. http://www.linux-kvm.org/.

[Sha] Microsoft Office SharePoint Server 2007. http://office.microsoft.com/de-de/sharepointserver/FX100492001031.aspx.

[Shi] Shibboleth. Web Single Sign-On. http://shibboleth.internet2.edu/.

[svn] Apache Subversion. http://subversion.apache.org/.

[VMw] VMware. VMware Virtualization Software for Desktops, Servers & Virtual Machines for a Private Cloud. http://www.vmware.com/.

[Wik] Wikipedia, the free encyclopedia. List of Collaborative Software. http://en.wikipedia.org/wiki/List_of_collaborative_software.

Netz-Design

Virtual Software Routers: A Performance and Migration Study

Zdravko Bozakov

zdravko.bozakov@ikt.uni-hannover.de

Abstract: It is expected, that the application of the virtualization paradigm to network resources can provide the basis for a Future Internet architecture and stimulate the introduction of novel protocols, services, and business cases. As a starting point for further research, we analyze the routing performance of a software router executed within different open source virtualization solutions, and evaluate the applicability of existing live-migration mechanisms to virtual routers.

1 Introduction

Network virtualization is an emerging technology, which has the potential to address the ossification of the current Internet architecture and become a fundamental building block for the Future Internet. In addition to allowing the operation of independent, parallel virtual networks, e.g. for Infrastructure as a Service (Iaas), virtual routers can be employed for the gradual introduction of new network protocols into existing infrastructures. In the network management domain, a major advantage of virtualized network resources, is the capability to transparently transfer logical router instances between physical routers. ISPs can utilize this feature, to adapt their infrastructure to changing traffic conditions, customer requirements or for energy conservation during off-peak hours.

While proprietary router virtualization solutions, such as logical routers, Virtual Device Contexts (VDC) or Virtual Routing and Forwarding (VRF), are available today, they are too limited in terms of interoperability and flexibility to serve as a basis for a virtual network architecture. Neither router migration, nor the execution of unsupported routing processes is currently possible. Due to the closed nature of commercial offerings, it is likely that research into router virtualization will be confined to open software platforms, at least for the near future.

To this end, we evaluate open source system virtualization solutions with respect to their routing performance, and their potential to serve as a starting point for further research in the network virtualization domain. Furthermore, we analyze the feasibility of existing virtualization technology as a basis for live router migration, and investigate the impact of router mobility on network traffic.

2 Related Work

Currently, several virtualization platforms are freely available under open-source licenses, including Xen, OpenVZ, KVM and VirtualBox. The performance level of all solutions has improved steadily, enabling the execution of virtual servers at near native speeds. As a result, today virtualization plays a major role for resource consolidation in data centers. However, I/O performance and the virtualization of network devices in particular, constitute a bottleneck and remain an open research field [AMN06, EGH+07]. An evaluation of Xen for network virtualization has been conducted in [MCZ06]. The concept of router migration as a management primitive was first advocated in [WKB+08], where the authors outline an architecture for control plane migration based on virtual machines (VM). Building upon these findings, we quantify the effects of migration mechanisms on the network, examine the network performance of Xen, KVM and OpenVZ, taking recent developments of the software suites into account.

2.1 System Virtualization Approaches

Paravirtualization, full virtualization and container-based virtualization are the three currently prevalent system virtualization approaches.

The Xen [BDF+03] virtual machine monitor (VMM), enables the execution of multiple guest operating systems on a single host machine by providing an abstraction of the underlying hardware. The Xen architecture is comprised of layers, known as domains, with the VMM (or hypervisor) running in the lowest and most privileged domain. The VMM is responsible for instantiating guest domains and managing system resources. Guest hosts require a kernel specifically modified to utilize the interfaces offered by the VMM. A major advantage of paravirtualization approach used by Xen, is the strict VM isolation, as well as the low performance penalty in guest domains which results from the adapted guest kernels. Additionally, the use of virtualization aware network drivers leads to significantly higher network performance. Furthermore, recent versions of Xen also support the virtualization of unmodified guests on CPUs providing hardware virtualization support.

The Kernel-based Virtual Machine (KVM) [KKL+07] project is a full virtualization implementation for Linux. In contrast to Xen, KVM is implemented as a loadable kernel module, which relies exclusively on hardware virtualization extensions, such as Intel VT-x or AMD-V. As a result, no guest-side modifications are necessary: each VM can be regarded as a Linux process executing in a special guest mode. Scheduling is performed using standard Linux mechanisms. On the downside, all guest I/O requests are trapped and emulated in user space by a dedicated process (QEMU), resulting in poor performance for I/O intensive operations. Recently, the availability of paravirtualized network drivers [Rus08] have led to significant improvements in KVM network and disk performance. In contrast to Xen, KVM is included in the main-line Linux Kernel, and can therefore benefit from short development cycles and frequent kernel optimizations.

A more lightweight virtualization strategy is implemented in OpenVZ [ope10]. In con-

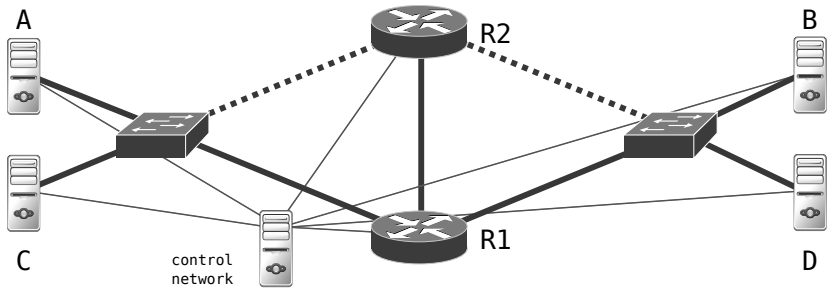


Abbildung 1: Experimental setup

trast to Xen and KVM, OpenVZ provides virtual environments (VE) which share the host machine's kernel. Guest system calls are passed through to the host kernel, creating the illusion of a standalone Linux system, with isolated resources. OpenVZ offers quotas, which can be used to control the allocation of physical resources. Even though VEs are not a true virtualization solution, they can be checkpointed and migrated across physical machines. The reduction of processing overheads, is the main motivation behind this approach.

3 Applications of Virtualization in Routers

From a network operator's viewpoint, two main advantages of network virtualization are the ability to support multiple concurrent networks, each potentially running different protocols, as well as increased flexibility resulting from the decoupling of physical and logical network entities.

Depending on the use-case requirements, different elements of a router architecture can be virtualized.

A prerequisite for live router migration, is the strict separation of control and forwarding planes. A router control plane running within a virtual environment (VE) can hence be transparently migrated while the data plane continues to forward traffic, as outlined in [WKB+08]. In order to ensure that network operation is not disrupted, for instance by dropped route update messages, it is vital to minimize the control plane downtime during the migration process.

Moreover, virtualization mechanisms can be employed to increase router availability. A possible approach consists of using control plane VE snapshots to ensure a quick router recovery e.g. after a crash. Additionally, it is conceivable that fallback control plane instances can be operated concurrently on separate hardware platforms, by suitably modifying existing migration mechanisms. The use of virtualized routers for testing alternative router configurations has also been proposed in [AWY08].

To operate isolated, concurrent networks on the same hardware substrate, the forwarding plane design must be adapted to support virtualization. High performance and efficient

sharing of hardware resources are key requirements in this case. At the same time, a virtual forwarding plane should be expandable, in order to support a wide range of protocols - a level of flexibility similar to system virtualization is desirable. The recently proposed OpenFlow [MAB+08] framework, is a highly promising approach for data plane virtualization. A different architecture has been proposed in [AF09].

Finally, a straightforward but highly demanding approach consists of executing an entire router within a virtualized environment. It can be expected, that due to the performance penalty associated with virtualization, the real-world use of fully virtualized routers will be limited in the foreseeable future. Nevertheless, we believe such a setup serves as a means to identify existing technologies which can be adopted for future use in specialized network virtualization solutions. Therefore, this option is evaluated in this paper.

3.1 Live Migration

The most basic VM migration strategy involves creating a VM snapshot (checkpointing), stopping VM execution, transferring the VM snapshot to a destination host, and resuming execution there. This approach, commonly referred to as *stop-and-copy*, is employed by OpenVZ [MKK08]. The downside of this mechanism is that it introduces a significant network downtime, approximately equivalent to the time needed to transfer the allocated VM memory over a link with a given capacity.

Xen employs a so-called *iterative pre-copy* migration mechanism followed by a *stop-and-copy* step [CFH+05]. When a migration is initialized, the guest's entire memory content is transfered to the destination host, and logging of modified (dirty) memory pages is enabled on the source VM. While the source VM continues to execute, pages modified since the beginning of the migration are iteratively copied to the destination VM until the number of dirty pages falls below a pre-defined threshold or a time limit is reached. Xen dynamically adjusts the migration transfer rate in order to minimize the disruption of the network. In the final step, the source VM is stopped, and the remaining dirty pages are copied to the destination VM at maximum speed. Ideally, this final working set should make up a fraction of the entire memory content, resulting in minimal network downtime. In this work we aim to quantify this disruption.

A similar approach is used in KVM. However, as shown in the results section, the implementation details are different.

For the remainder of this paper, we focus on the migration mechanisms of Xen and KVM.

4 Experimental Setup

We used the setup depicted in Fig. 1 to evaluate the routing performance of virtualized software routers and the effects of live migration on network traffic. Four nodes were connected by Gigabit Ethernet links, and additionally attached to a separate control net-

work. Nodes A and B act as a UDP traffic source and sink respectively. As it is not possible to saturate a Gigabit link using commodity hardware and operating systems, we utilized NetFPGA cards as traffic generators. The NetFPGA packet generator [CGLM09] is capable of transmitting 64 byte packets at line rate. A XORP software router [HHK03] was started within a VM/VE on node R1 and was subsequently migrated to R2 over a dedicated link. We believe, that the assumption of dedicated resources for router migration is realistic for network operation centers. Each VM was assigned 256 MB RAM and a single CPU core. R1 and R2 were booted from a live-CD, eliminating the need for a shared file-system. In addition, we measured the round-trip time (RTT) between nodes C and D before and during the migration process.

We used Xen version 3.2.1, KVM version 84 and OpenVZ version $1.2133\_FC5.026$. Dell Optiplex 760 with Q8400 Core 2 Quad CPUs and 4GB RAM were used for nodes R1 and R2. The nodes were equipped with Quad Port Intel PRO/1000 network cards. Each network interface was bound to a dedicated Linux bridge.

All measurements were automated using [BB08] and repeated 25 times. 95% confidence intervals are included in all plots.

5 Results

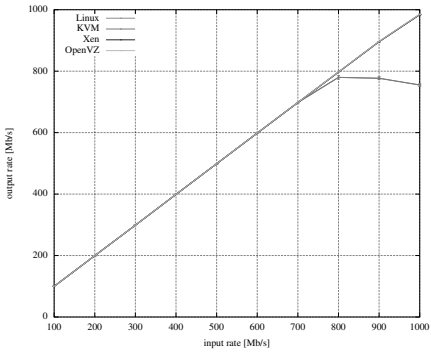
5.1 Virtual Machine Forwarding

We measured the performance penalty associated with routing packets within a VM, by comparing input and output packet rates. We used constant bit rate, UDP cross-traffic consisting of maximum and minimum sized Ethernet packets (1500B and 64B respectively). As a baseline the forwarding performance of a bare Linux system was also measured.

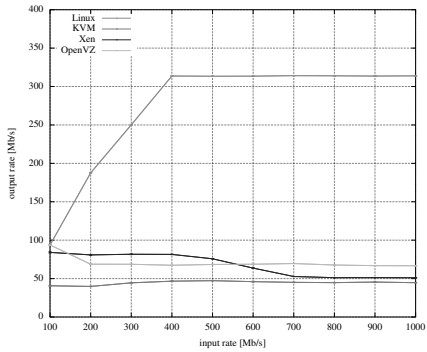
All evaluated virtualization approaches rely on Linux bridging to provide network connectivity to VMs. KVM and OpenVZ utilize user space virtual network devices (TAP) to the enable access to the network hardware, while the Xen hypervisor provides dedicated kernel space interfaces.

With large cross-traffic packets the forwarding performance of Linux, Xen and OpenVZ, was identical and sufficient to fully saturate the Gigabit link. Using the *virtio* network driver, KVM was able to fill almost 80% of the link. In contrast, the fully virtualized Intel *e1000e* driver, KVM performance was extremely poor at ~ 5Mbps.

While Linux forwarding was able to achieve slightly over 300 Mbps using small packet cross-traffic, all virtualization approaches achieved significantly lower throughput speeds. It is interesting to note that the forwarding performance of Xen and OpenVZ deteriorates after 500Mbps and 100Mbps respectively. KVM throughput was constant at only $\sim 5\%$ of the link capacity. Analysis of the traces showed that in all cases, the discrepancy between the Linux and VM throughput values is mainly due to packet loss between the physical input interface and the bridged virtual interface, rather than loss withing the VM. This implies, that the Linux bridging system might be the cause for significant packet loss.

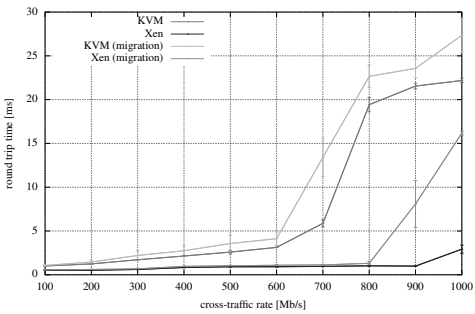


(a) 1500B packet cross-traffic

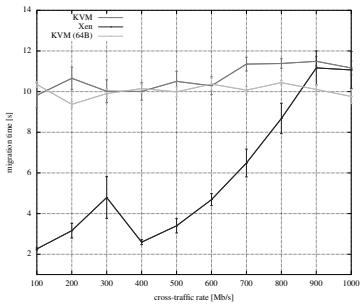


(b) 64B packet cross-traffic

Abbildung 2: Forwarding performance



(a) Packet round trip time



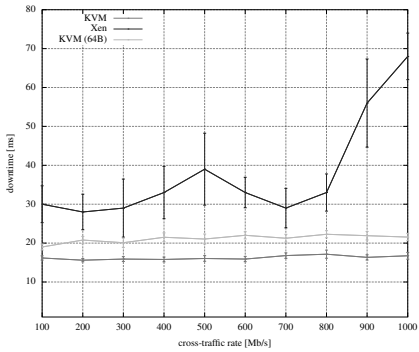
(b) Migration duration

In addition, we measured the performance of Xen's PCI pass-through capability, which allows for network devices to be assigned exclusively to a virtual machine. Results were identical to the pure Linux forwarding case and are not shown here.

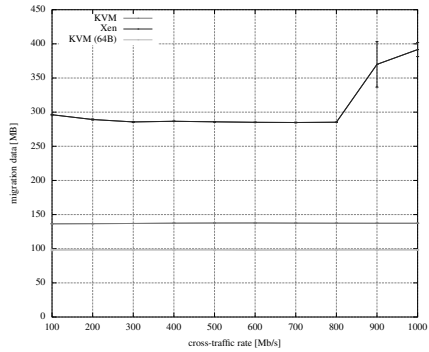
The forwarding results, are depicted in Fig. 2. Additionally, Fig. 3a shows the round trip time dependency on the cross-traffic.

5.2 Live-Migration Effects

A dedicated link between R1 and R2 was used for the migration traffic, in order to examine the influence of the migration process on the network. Migration while forwarding small cross-traffic packets proved a challenging task for both Xen and KVM. The Xen migration process failed repeatedly, even leading to reproducible lockups of the virtual machine. This poses a significant problem, limiting the usability of Xen migration in real-world scenarios.



(a) Migration downtime



(b) Migration traffic volume

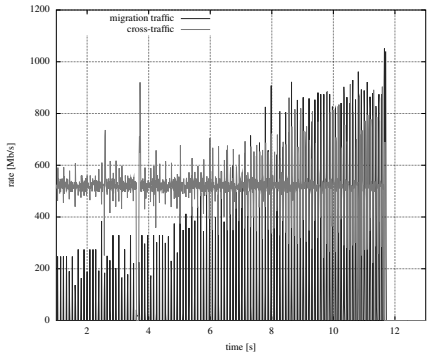
In the following, we only present results for large packet cross-traffic under Xen.

The migration process at R1 for KVM and Xen for 500Mbps and 1000Mbps cross-traffic respectively are exemplified in Fig. 3. The migration is initiated at time 0, with the stop-and-copy peak visible in the right end of each migration traffic curve. Traffic data was collected using the Linux *proc* packet counters, with 10ms resolution. It is notable, that the total length of the migration process appears reasonably constant for KVM. The migration is performed as a series of bursts, of increasing transfer rates, each followed by a inactivity period. As the migration progresses, the migration rate increase, adversely affecting the cross-traffic rate. In contrast, using Xen the migration traffic rate correlates with the intensity of the cross traffic, resulting in shorter migration times at low cross-traffic rates.

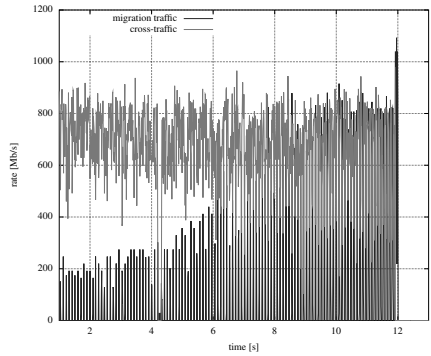
These notions are confirmed by our series of automated experiments. For both virtualization approaches, we measured the total duration of the migration process, the network downtime caused by the stop and copy phase, and the bandwidth generated by the migration. Using Xen, the total duration time of the migration showed a dependency on the cross traffic intensity, ranging from 2s up to 12s. An unexpected increase in the migration time can be observed at a cross-traffic rate of 300Mbps. For the KVM migration implementation, no significant cross-traffic dependency was apparent. The results are depicted in Fig. 3b.

The network downtime introduced by the final stop and copy migration phase was independent of the cross-traffic at ≈ 0.17s for KVM and highly variable for Xen ranging from 3s to 7s. For small packet cross traffic the KVM downtime is slightly higher than for large packets. The relationship is shown in Fig. 3a.

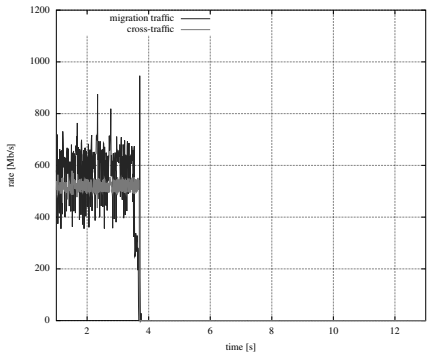
Fig. 3b shows the total amount of data transferred during the VM migration. Using Xen, the migration traffic is slightly higher than the allocated memory for the VM. At 900Mbps cross-traffic, the amount of data increases significantly. It is evident, that the migration traffic volume can not fully account for the increase in migration time. Hence, the behaviour visible in Fig. 3b must be due to Xen's migration rate adaptation mechanism.



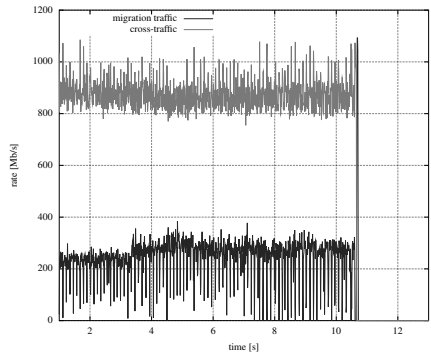
(a) KVM: 500Mbps cross-traffic



(b) KVM: 1000Mbps cross-traffic



(c) Xen: 500Mbps cross-traffic



(d) Xen: 1000Mbps cross-traffic

Abbildung 3: Migration process samples

For KVM no notable increase in the amount of transferred data is evident. It is noteworthy, that the constant data volume of ≈ 140MB is less than the size of assigned VM memory.

Additionally, the round trip increase during the migration process is plotted in Fig. 3a. As expected, the RTTs increase as the cross-traffic intensity rises. For Xen, an exceptionally large increase occurs at cross-traffic speeds larger than 800Mbps.

6 Conclusion

Our evaluation showed, that the performance of the Linux network stack running on commodity hardware is insufficient to serve a full Gigabit network link using minimum sized Ethernet packets. Not surprisingly, the virtualization layers generate additional packet pro-

cessing overhead, leading to further performance deterioration. Regardless of the utilized virtualization approach, the penalty on network throughput for small packet sizes remains extremely high. Moreover, under such conditions, the Xen migration process did not complete reliably in a significant number of cases. This constitutes a major obstacle for the utilization of Xen based migration of software routers in real-world scenarios.

Nevertheless, examining traffic with larger packet sizes showed that the forwarding performance was acceptable for Linux as well as all virtualization approaches. Among the evaluated solutions, Xen delivers the best forwarding performance for small Ethernet packets. KVM's full virtualization architecture, combined with paravirtualized network drivers achieves results almost comparable to Xen. Surprisingly, in terms of network performance, OpenVZ's lightweight, container-based architecture does not achieve significant improvements and is on par with Xen. Further work is required to verify indications that the Linux bridging system represents a bottleneck in the system, as all evaluated approaches rely on it to provide connectivity between physical and virtual network devices.

We confirmed that the simple migration mechanism employed in OpenVZ leads to significant downtimes, and that extremely short network disruptions can be achieved using the iterative stop and copy migration mechanism. Assuming migration stability issues are addressed in future software versions, the migration functionality of both Xen and KVM can be applied for applications with moderate throughput requirements. The migration of the control plane of a software router represents a feasible scenario. However, we expect that dedicated hardware support is essential for the implementation of a high performance forwarding-plane in virtual routers. In future work, we aim to present a migratable virtual router platform, with an OpenFlow based data plane, where the controller responsible for computing routing tables is executed within a virtual environment.

Literatur

[AF09] Muhammad Bilal Anwer und Nick Feamster. Building a fast, virtualized data plane with programmable hardware. In *VISA '09: Proceedings of the 1st ACM workshop on Virtualized infrastructure systems and architectures*, pages 1–8, New York, NY, USA, 2009. ACM.

[AMN06] P. Apparao, S. Makineni und D. Newell. Characterization of network processing overheads in Xen. *Virtualization Technology in Distributed Computing, 2006. VTDC 2006. First International Workshop on*, pages 2–2, Nov. 2006.

[AWY08] Richard Alimi, Ye Wang und Y. Richard Yang. Shadow configuration as a network management primitive. *SIGCOMM Comput. Commun. Rev.*, 38(4):111–122, 2008.

[BB08] Zdravko Bozakov und Michael Bredel. SSHLauncher - A Tool for Experiment Automation. Technical report, TU-Darmstadt, 2008.

[BDF+03] Paul Barham, Boris Dragovic, Keir Fraser, Steven Hand, Tim Harris, Alex Ho, Rolf Neugebauer, Ian Pratt und Andrew Warfield. Xen and the art of virtualization. In *SOSP '03: Proceedings of the nineteenth ACM symposium on Operating systems principles*, pages 164–177, New York, NY, USA, 2003. ACM Press.

[CFH+05] Christopher Clark, Keir Fraser, Steven Hand, Jacob Gorm Hansen, Eric Jul, Christian Limpach, Ian Pratt und Andrew Warfield. Live migration of virtual machines. In *NSDI'05: Proceedings of the 2nd conference on Symposium on Networked Systems Design & Implementation*, pages 273–286, Berkeley, CA, USA, 2005. USENIX Association.

[CGLM09] G.A. Covington, G. Gibb, J.W. Lockwood und N. Mckeown. A Packet Generator on the NetFPGA Platform. In *Field Programmable Custom Computing Machines, 2009. FCCM '09. 17th IEEE Symposium on*, pages 235–238, April 2009.

[EGH+07] N. Egi, A. Greenhalgh, M. Handley, M. Hoerdt, L. Mathy und T. Schooley. Evaluating Xen for Router Virtualization. *Computer Communications and Networks, 2007. ICCCN 2007. Proceedings of 16th International Conference on*, pages 1256–1261, Aug. 2007.

[HHK03] Mark Handley, Orion Hodson und Eddie Kohler. XORP: an open platform for network research. *SIGCOMM Comput. Commun. Rev.*, 33(1):53–57, 2003.

[KKL+07] Avi Kivity, Yaniv Kamay, Dor Laor, Uri Lublin und Anthony Liguori. kvm: the Linux Virtual Machine Monitor. In *Proceedings of the Linux Symposium*, June 27th–30th 2007.

[MAB+08] Nick McKeown, Tom Anderson, Hari Balakrishnan, Guru Parulkar, Larry Peterson, Jennifer Rexford, Scott Shenker und Jonathan Turner. OpenFlow: enabling innovation in campus networks. *SIGCOMM Comput. Commun. Rev.*, 38(2):69–74, 2008.

[MCZ06] Aravind Menon, Alan L. Cox und Willy Zwaenepoel. Optimizing Network Virtualization in Xen. In *In Proc. USENIX Annual Technical Conference (USENIX 2006)*, pages 15–28, 2006.

[MKK08] Andrey Mirkin, Alexey Kuznetsov und Kir Kolyshkin. Containers checkpointing and live migration. In *Proceedings of the Linux Symposium*, July 23rd–26th 2008.

[ope10] OpenVZ. http://www.openvz.org, January 2010.

[Rus08] Rusty Russell. virtio: towards a de-facto standard for virtual I/O devices. *SIGOPS Oper. Syst. Rev.*, 42(5):95–103, 2008.

[WKB+08] Yi Wang, Eric Keller, Brian Biskeborn, Jacobus van der Merwe und Jennifer Rexford. Virtual routers on the move: live router migration as a network-management primitive. *SIGCOMM Comput. Commun. Rev.*, 38(4):231–242, 2008.

Netzentwicklungskonzept für ein großes Universitätsnetzwerk – Bestandspflege und Erschließung neuer Technologien

Dr. Raimund Vogl, Markus Speer, Norbert Gietz, Ludger Elkemann

Zentrum für Informationsverarbeitung
Westfälische Wilhelms-Universität Münster
Röntgenstraße 9 - 13
48149 Münster
rvogl@uni-muenster.de, speer@uni-muenster.de,
gietz@uni-muenster.de, elkeml@uni-muenster.de

Abstract: Die Westfälische Wilhelms-Universität Münster (WWU) ist eine der größten Universitäten in Deutschland und mit ihren über 200 Gebäuden weiträumig über das Stadtgebiet verteilt – ein gut ausgebautes und hoch verfügbares Kommunikationssystem ist folglich von zentraler Bedeutung für die effiziente Unterstützung der Prozesse in Forschung, Lehre und Administration. So hat sich in den zurückliegenden 6 Jahren die Zahl der LAN-Anschlüsse im Netz der WWU auf über 26.500 (mit den Anschlüssen im integrierten Netz des Universitätsklinikums Münster (UKM) sogar über 43.000) mehr als verdoppelt. Mit der Integration des TK/AVM-Bereichs der Universitätsverwaltung in das Zentrum für Informationsverarbeitung (ZIV) Anfang 2008 und dem damit verbundenen Bedarf für die synergetische Umsetzung der Konvergenz der Kommunikationssysteme, mit dem immer rascher anwachsenden Bedarf für 10GE Ports in den Data Centers und der Notwendigkeit für umfangreiche Erneuerungen bei den aktiven Netzwerkkomponenten (im Edge wie auch im Core) war die Erstellung eines neuen, langfristigen Netzentwicklungskonzeptes notwendig. In einem intensiven Diskussionsprozess wurden dabei die Grundlagen für zahlreiche strategische Entscheidungen erarbeitet und die Gesichtspunkte der IT-Sicherheit, eines einfach handhabbaren personalsparenden Netz-Managements und der von Nutzerseite dringend gewünschten mobilen Konnektivität berücksichtigt.

1 Die Ziele des Netzentwicklungskonzeptes der WWU Münster

Information hat sich in den letzten Jahrzehnten zum zentralen Faktor für ein erfolgreiches Arbeiten in allen Bereichen der Wirtschaft und des öffentlichen Lebens entwickelt. Vom Fluss der Informationen, und von der Funktionsfähigkeit der Systeme zur Informationsverarbeitung hängt inzwischen die Arbeitsfähigkeit moderner Organisationen ab. Insbesondere zuverlässige und weitum verfügbare Datennetzwerke sind dafür die Grundvoraussetzung. Sie bilden die Infrastruktur für die Forschung im Sinne von „eScience“ und unterstützen die Gestaltung neuer, zukunftsorientierter Lehr- und Lernumgebungen.

Insbesondere für Universitäten ohne homogene Campus-Struktur stellt der Auf- und Ausbau eines umfassenden Kommunikationssystems einen bedeutenden personellen und finanziellen Faktor dar. Die Westfälische Wilhelms-Universität Münster (WWU) hat schon sehr früh mit einem umfangreichen Ausbau der Netzwerkinfrastruktur begonnen und konnte eine sehr weitreichende Abdeckung erreichen – aktuell kann von Vollausbau gesprochen werden. Die Kompetenzen für Ausbau und Betrieb des Netzwerkes der WWU wie auch des Universitätsklinikums Münster (UKM) sind klar geregelt und ausschließlich in der Verantwortung des Zentrums für Informationsverarbeitung (ZIV) der WWU.

Mit der Ausarbeitung eines neuen, langfristigen Netzentwicklungskonzeptes wird zentral das Ziel verfolgt, auch bei beträchtlichen Fluktuationen im weitverstreuten Gebäudebestand der WWU diesen Status des Vollausbaus zu erhalten und einen höchst zuverlässigen Betrieb des Kommunikationssystems, der allen zukünftigen Leistungsanforderungen gerecht wird, zu gewährleisten. Das Kommunikationssystem darf kein limitierender Faktor für die zukünftige Entwicklung der WWU Münster in Forschung und Lehre sein.

Dabei sind die Hauptziele:

- **Konvergenz:** Zusammenführung von Telekommunikations-, Daten- und Speichernetzwerk in technischer und personeller Sicht.
- **Verfügbarkeit:** höchste Zuverlässigkeit und umfassende Abdeckung aller Bereiche der WWU durch das Kommunikationssystem.
- **Leistungsfähigkeit:** proaktive Adressierung absehbarer Leistungs-Anforderungen zur Verhinderung behindernder Engpässe bei laufendem Wachstum.
- **Sicherheit:** Gewährleistung eines Höchstmaßes an Datensicherheit durch organisatorische Sicherheitsmaßnahmen, netzseitige Sicherheitseinrichtungen und Netzdienste für Datenhaltung und Sicherung.
- **Effizienz:** Optimierung der User-Helpdesk- und der User-Self-Care-Mechanismen

Dabei wird das Kommunikationssystem in seiner Gesamtheit adressiert – nicht nur das Datennetzwerk, sondern auch die Telekommunikation (TK) und sonstige Netzdienste. Die vorgestellten Konzepte gelten aber genauso für das ebenfalls vom ZIV betreute und voll integrierte Kommunikationssystem des UKM. Die dargestellten Planungen beziehen sich auf einen Zeitraum von ca. 7 Jahren (d.h. bis ca. 2017). Dieser Planungszeitraum wird bewusst gewählt, da dies einem realistischen kompletten Innovationszyklus bei den aktiven Netzwerkkomponenten entspricht, der nur bei dieser Laufzeit mit den verfügbaren internen Personalressourcen bewältigt werden kann.

2 Bedarfsbegründende Grunddaten

Die WWU zählt zu den sehr großen Hochschulen in Deutschland mit Schwerpunkten in den Geistes- und Sozialwissenschaften, den Gesellschaftswissenschaften, den Naturwissenschaften und der Medizin; die Ingenieurwissenschaften sind nicht vertreten. 15 Fachbereiche bilden die organisatorischen Grundeinheiten der WWU. In über 110 Studienfächern mit 250 Studiengängen gab es im Wintersemester 2008/09 ca. 37.000 Studierende. Die Zahl der jährlichen Absolventen liegt bei ca. 5.500. Die ca. 5.000 Beschäftigten der WWU setzen sich wie folgt zusammen: 565 Professoren, 2.700 Wissenschaftliche Mitarbeiter, und 1.700 weitere Mitarbeiter. Bei der WWU handelt es sich um eine über die ganze Stadt Münster verteilte Flächenuniversität. Das Kommunikationsnetz der WWU ist daher ein typisches Metropolitan Area Network (MAN). Mit der flächendeckenden Erschließung aller Gebäude über das universitätseigene ca. 230 km umfassende Glasfasernetz ist ein hoher Aufwand verbunden. Das Kommunikationsnetz umfasst LAN-, traditionelle TK-Technologien, und weitere gebäuderelevante Technologien wie Gebäudeleittechnik, Sicherheits- und Zugangstechnik.

Kennzahl	**Wert**
Gebäude	212
Räume	15.340
Gesamtlänge des LWL-Netzes (WWU+UKM)	229 km
registrierte Nutzerkennungen	57.600
LAN-Verteilerstandorte	218
Netz-Anschlussdosen	28.082
WLAN Access Points	732
registrierte LAN-Endsysteme	15.971
Core/Midrange Router/Switches	15
Distribution/Edge-Switches (WWU+UKM)	ca. 2.000
(aktive) TK-Nebenstellen	8.490
TK-Standorte	47
VoIP-Telefone	470

Tabelle 1: Kennzahlen des Kommunikationssystems der WWU

3 Maßnahmenplan für Erneuerung und Ausbau

Der große Umfang des Kommunikationssystems erfordert substantielle Aufwände für die Erhaltung der Infrastruktur (insbesondere proaktiver Austausch der aktiven Komponenten nach maximal 7 Jahren Nutzungszeit zur Gewährleistung der betrieblichen Stabilität und Bereitstellung aktueller Funktionalitäten und Leistungsmerkmale). Trotz des bereits erreichten hohen Abdeckungsgrades ist weiterhin ein ungebrochenes Wachstum des Kommunikationsnetzes mit über 3.000 Neuanschlüssen pro Jahr zu erwarten, das teils aus der forcierten Installation von

WLAN-Access-Points, teils aus der Nutzung von Cat6 für TK-Verkabelung bei allen neuen Bauprojekten resultiert. Für den Zeitraum bis 2017 wird – nicht zuletzt wegen der sukzessiven Migration der TK-Anschlüsse – ein unverändertes Aufkommen an Neuanschlüssen in dieser Größenordnung erwartet.

Auf Grund dieses Mengengerüstes ist klar, dass der Ausbau und die Erneuerung des Netzwerkes nur kontinuierlich und nicht in disruptiven Projektschritten erfolgen kann – die personellen Kapazitätsanforderungen und die logistischen Voraussetzungen dafür wären zu groß und die Gefahren für eine nicht tolerierbare Beeinträchtigung des Netzbetriebs zu hoch. Insbesondere der Ausbau der Netzanschlüsse, die Verbesserung des House-Keepings, der Ausbau des WLAN, der Austausch der Edge-Switches erfolgen dabei kontinuierlich.

Die zentralen Maßnahmen, die zur Erreichung der eingangs genannten Hauptziele umgesetzt werden sollen sind in ihrer zeitlichen Abfolge bereits recht gut umreißbar:

- vollständige Umsetzung des 3-Layer-Core-Schemas (insb. 10GE-Anbindung des Distribution-Layers an den Midrange) und damit einhergehend der Ersatz der Multimode- durch Singlemode-Verkabelung im Laufe der Jahre 2010-2012
- Umstellung auf 40GE-Technologie in Core und Midrange in 2012-2014
- Etablierung von Data Center Switches in 2012
- vollständige Abstützung der audiovisuellen Medientechnik über das LAN und Schaffung einer zentralen Management- und Wartungsplattform bis 2014
- flächendeckende WLAN-Versorgung mit 802.11n bis 2015
- flächendeckende Bereitstellung von 1GE und Einführung von 802.1x bis 2016
- flächendeckende Einführung von VoIP und Ablösung der TDM TK Komponenten bis 2017

Begleitend dazu ist die Pflege und Erweiterung der Funktionalitäten zur Netzwerk-Administration und Dokumentation (zentral und mandantenfähig dezentral), für Netzwerk-Monitoring und für die Netzwerk-Sicherheit geplant.

4 Netzkonzept: vorhandene und angestrebte Netzstruktur

4.1 Grundzüge des Netzdesigns

Das Netzdesign der WWU wird von den Grundsätzen der Verfügbarkeit und der in das Netz eingebetteten Sicherheit bestimmt. Im Rahmen der Verfügbarkeit wird nicht auf eine erhöhte Einzelgeräteverfügbarkeit durch z.B. redundante Module sondern auf eine Doppelung der Geräte und Funktionen an unterschiedlichen Standorten gesetzt. Um sich auch bei der Stromversorgung auf unterschiedliche Quellen abzustützen zu können, werden jeweils 2 Netzteile eingesetzt. Lediglich im Edge wird im Allgemeinen auf diese Redundanzen verzichtet. Durch die ins Netzwerk eingebetteten IT-

Sicherheitsmaßnahmen wird das Gefährdungspotenzial für ganze Netzbereiche erheblich reduziert (vgl. Detaildarstellung unter 4.3). Folgende aufeinander hierarchisch aufbauende Netzbereiche werden unterschieden (siehe auch Abb. 1):

- **Edge:** Anbindung von Endsystemen, nur Layer2-Funktionalität
- **Distribution:** 16 Standorte, Aggregieren von Edge-Devices, nur Layer2-Funktionalität, Einführung dieses Bereiches um kostengünstig 10GE einsetzen zu können, Server-Anbindung
- **Midrange:** 6 Standorte, Aggregieren von Distribution-Devices großer Netzbereiche, zukünftig Anbindung von Data Centern, Layer3/IP-Funktionalität, Paketfiltering
- **Core:** 2 Hauptstandorte, Kopplung der Midrange-Bereiche, Layer3/IP-Funktionalität, Realisierung zentraler Netzfunktionen (WLAN-Switching, zentrale Security-Funktionen: Paketfilter, Firewall-Funktionalität, Intrusion-Prevention, VPN)
- **Inter-Core:** 2 Standorte zur Layer3-Kopplung der Netze der verschiedenen Einrichtungen (WWU, UKM, FH, MPI) zum WNM (Wissenschaftsnetz Münster)

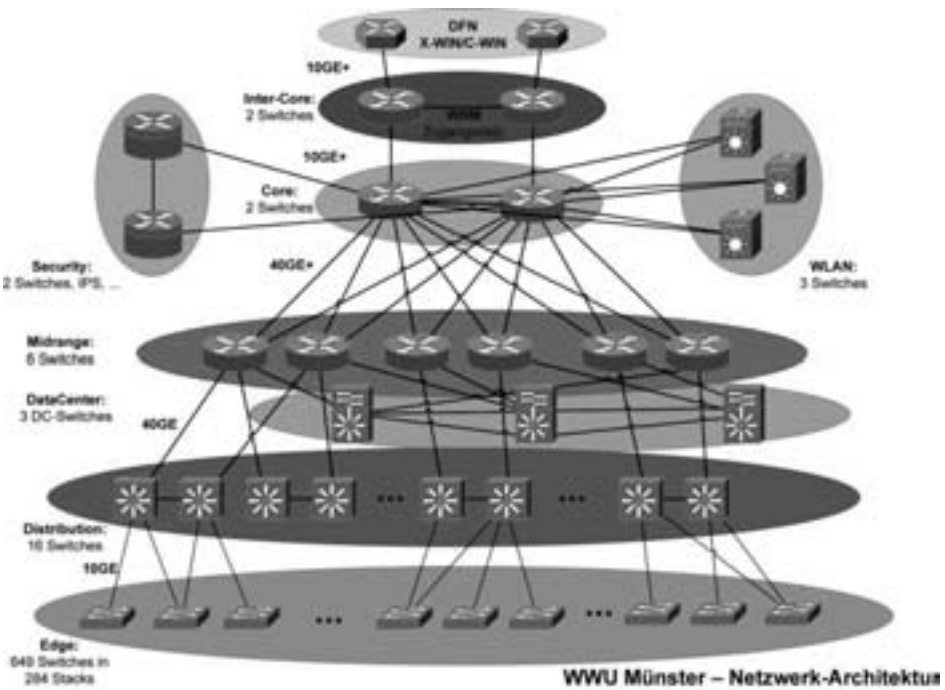


Abb.1: Schematische Darstellung der Architektur mit Core (samt zentraler Security und WLAN Switching) – Midrange (samt Data Center) – Distribution – Edge

Zur Erhöhung der Verfügbarkeit sollen einzelne Edge-Bereiche über ein Paar von Distribution-Switches angebunden werden (siehe Abb. 1). Jeder Edge-Switch wird im Normalfall mit einem der beiden der Distribution-Switches verbunden. Nur ca. 20 % der Edge-Switches mit erhöhten Verfügbarkeitsanforderungen werden mit beiden Distribution-Switches verbunden. Die Distribution-Switches sollen untereinander verbunden und jeweils eine Verbindung zum übergeordneten Midrange-Switch besitzen wodurch dieser Netzbereich redundant angebunden ist. Ein Midrange-Switch hat je eine Verbindung zu einem der Core-Switches. Die Core-Switches sind untereinander verbunden. Die Data Center sollen als Ring untereinander verbunden und jeweils an 2 Midrange-Switches angeschlossen werden.

Das Netz stützt sich auf die 2 Hauptstandorte in der Einsteinstraße und Röntgenstraße ab. An diesen Standorten sind insbesondere die Core- und Inter-Core-, aber auch die lokalen Midrange- und Distributionsfunkionalitäten realisiert. Als Gerätetyp kommt im Inter-Core, Core und Midrange ausschließlich der Cisco C6509 zum Einsatz. Im noch weitgehend zu realisierenden Distribution-Bereich soll hingegen der Gerätetyp HP 5412zl eingesetzt werden. Im Edge kommen aktuell Geräte der Hersteller HP, 3Com und Nexans zum Einsatz. Im Rahmen der internen Herstellerpolitik soll auch zukünftig eine alleinige Herstellerbindung vermieden und der Wettbewerb zwischen den Herstellern aufrechterhalten werden.

Das beschriebene Konzept ist bereits im Core- und Midrange-Bereich umgesetzt worden. Die Implementierung des Distribution-Bereichs ist bislang exemplarisch in einigen Bereichen vorgenommen worden. Die netzweite Umsetzung dieses Konzepts ist allerdings eine noch zu leistende umfangreiche Aufgabe. Darüber hinaus müssen die absehbaren Bandbreitenanforderungen durch leistungsfähige Verbindungen (10GE, Nx10GE, später 40GE bzw. 100GE) zwischen den Netzbereichen abgedeckt werden.

4.2 Ausführliche Darstellung der Netzstruktur

4.2.1 Verkabelungsstruktur

Die Verkabelung im Tertiärbereich wurde bereits frühzeitig nach dem Cat5e- und später dem Cat6-Standard ausgeführt. Lediglich die ersten Verkabelungen in den 1990er-Jahren entsprechen nur Cat5, wobei bereits die seinerzeit verwendeten Leitungen den Anforderungen der heutigen Cat5e genügen und durch Umrüsten der Anschlusstechnik leicht gigabit-fähig gemacht werden können. Zur effizienteren Ausnutzung der aktiven Technik und des House-Keepings werden bei der strukturierten Verkabelung möglichst wenige Verteiler innerhalb eines Gebäudes angestrebt. Hierdurch entfällt eine Sekundärverkabelung weitestgehend. Im Primärbereich stützt sich das Netz größtenteils noch auf eine seit den 1980er gewachsenen Multi-Mode-Verkabelung ab. Diese soll durch eine Single-Mode-Verkabelung nach den folgenden Grundsätzen abgelöst werden:

- Im Normalfall wird ein Gebäude mit nur einem LWL-Kabel an einem Distributionsswitch-Standort angebunden

- In Einzelfällen wird für Gebäude mit erhöhten Verfügbarkeitsanforderungen (z.B. Lokationen mit zentralen Services, ...) eine redundante LWL-Anbindung angestrebt.
- Durch die Installation von VoIP-Endgeräten ergeben sich keine erhöhten Verfügbarkeitsanforderungen für die LWL-Anbindung dieses Gebäudes.
- Die beiden Distributionsstandorte eines Netzbereiches werden untereinander verbunden, diese LWL-Verbindung dient auch zum Durchschalten evtl. redundanter Edge-Anbindungen.
- Distributionsstandorte werden mit beiden zugehörigen Midrange-Standorten verbunden
- Midrange-Standorte werden mit beiden Core-Standorten verbunden
- Core-Switch-Standorte werden untereinander verbunden

4.2.2 Layer2-Strukturen

Auf Layer-2-Ebene wird die VLAN-Technologie eingesetzt. Dabei werden die Verbindungen zwischen den Netzwerkkomponenten grundsätzlich „tagged“ und die Verbindungen zu Endsystemen „untagged“ ausgeführt. Lediglich ausgewählte Server werden auch „tagged“ angebunden. Hierdurch ist es möglich die einzelnen VLANs über geografische Bereiche hinweg im gesamten Netz zu verteilen. Im Edge- und Distributionsbereich werden nur Layer-2-Funktionen eingesetzt. Nach Ihrer Funktion werden folgende VLAN-Typen unterschieden:

- Endnutzer-VLANs: Anschluss von Endgeräten (Clients, Server, VoIP-Telefone)
- Insel-VLAN: spezielle Endnutzer-VLANs als abgeschottete Bereiche
- Transfer-VLANs: Verbindung von IP-Routern (physischen und virtuellen)
- VPNSM-VLANs: für die direkte VPN-Einwahl in ein Endnutzer-VLAN

Das Routing auf Layer2 erfolgt mit der STP-Protokollfamilie (Spanning Tree Protocol). Dabei sind zwei voneinander unabhängige STP-Bereiche zu unterscheiden: Im Core/Midrange-Bereich wird Rapid PVST (Per VLAN Spanning Tree), im Distribution/Edge-Bereich wird RSTP (Rapid Spanning Tree Protocol) eingesetzt. Der Ansatz, die VLAN-Technologie intensiv zu nutzen, hat sich in der Vergangenheit bewährt und soll fortgeschrieben werden. Eine Konsequenz des oben erläuterten Konzepts ist ein großer Bedarf an VLANs der durch zukünftige und den Ausbau vorhandener Dienste (VoIP) weiter steigen wird. Durch das Aufteilen der VLAN-IDs in verschiedene Nummernräume (ID-Range) für einzelne Bereiche und Funktionalitäten (z.B. WWU, UKM, Data Center, Transfernetze) wird die Administrierbarkeit verbessert und die mehrfache unabhängige Verwendung von VLAN-IDs erleichtert.

4.2.3 Layer3-Strukturen

Layer3-Funktionen werden ausschließlich auf den Geräten im Midrange- und Core-Bereich etabliert. Hier lässt sich durch die Cisco-IOS-Funktion „VRF-lite“ die IP-Router-Funktionalität virtualisieren, wodurch eine Vielzahl von IP-Routing-Instanzen (kurz VR) auf einer Hardware definiert werden kann. Die VRs werden dabei sowohl für die Layer3-Anbindung von IP-Subnetzen für Endsysteme als auch für den Aufbau einer Hierarchie von VRs eingesetzt. Im Abschnitt 4.3 wird erläutert, wie hierdurch netzseitig eingebettete Sicherheitslösungen aufgebaut werden können. Auch bei den VRs wird dabei konsequent die Gerätedopplungsstrategie fortgesetzt, indem ein VR-Paar auf zwei Chassis aufgeteilt wird. Derzeit sind ca. 270 VRs (WWU und UKM) realisiert. Zur Erhöhung der Verfügbarkeit kommen HSRP, OSPF und BGP zum Einsatz. Dieses Layer3-Design hat sich in der Vergangenheit bewährt und soll fortgeschrieben werden. IP-Multicast und IPv6 sind noch nicht in substanziellem Umfang eingeführt. Dies soll zukünftig erfolgen.

4.2.4 Netztechnologien und Netzzugangstechnologien

Als Technologie zur Verbindung der Netzkomponenten kommt nahezu ausschließlich Ethernet zum Einsatz. Innerhalb des Core und Midrange wird derzeit ausschließlich 10GE-Technik eingesetzt. Abhängig von der Verfügbarkeit ist mittelfristig eine Hochrüstung auf 40GE-Technik vorzunehmen, alternativ ist hier auch zunächst eine Aggregation von 10GE-Verbindungen möglich. Die konsequente Einführung eines mit 10GE-Technologie angebundenen Distribution-Bereichs ist eine noch in großem Umfang zu realisierende Aufgabe. Bei den Downlink-Verbindungen vom Distribution-Bereich zum Edge-Bereich handelt es sich je nach Konstellation (Portdichte, Performance-Anforderungen) um 1GE, aggregierte 1GE oder 10GE-Verbindungen. Hier soll im Laufe der Jahre weitgehend auf 10GE-Technologie umgestellt werden. Vor kurzem wurde eine eigene DSL-Infrastruktur aufgebaut, um einfach und flexibel das vorhandene Kupferkabelnetz nutzen zu können, solange in Einzelfällen noch keine eigene LWL-Anbindung existiert oder diese unwirtschaftlich ist. Zu Standorten ohne eigene Leitungswege wird die DSL-Technik externer Anbieter genutzt.

Für den Zugang von Endgeräten zum Kommunikationssystem wird eine Reihe von Zugangstechnologien unterstützt:

- LAN-Festanschlüsse für registrierte Endsysteme
- „öffentliche“ LAN-Festanschlüsse mit VPN-Zugangsmöglichkeit
- VPN-Zugang aus externen Netzen
- dedizierter VPN-Zugang in eine bestimmte Netzzone (VLAN)
- WLAN (siehe 4.2.5)
- DSL/PPPoE

Der Netzzugang mit 802.1X an LAN-Festanschlüssen ist noch nicht in nennenswertem Umfang realisiert. Es ist geplant, diese Netzzugangstechnologie flächendeckend zu

etablieren. Der Nutzer soll sich dabei flexibel in eine bestimmte Netzzone „einwählen“ können. Hierfür müssen jedoch die älteren Edge-Switches erneuert werden. Beim externen VPN-Zugang soll zukünftig, dort wo die Installation einer VPN-Client-Software nicht akzeptabel ist, eine einfachere SSL-VPN-basierte Zugangsmethode implementiert werden.

4.2.5 WLAN

Derzeit sind zwei verschiedene für den Nutzer transparente WLAN-Installationen im Einsatz. Bei der älteren WLAN-Installation handelt es sich um eine Lösung der Firma Proxim mit autonomen Access Points (APs). Diese Installation ist immer noch in großem Umfang mit ca. 300 APs in Betrieb. Seit 2008 ist eine zentrale controller-basierte WLAN-Switching-Lösung der Firma Cisco, die sich im Core-Bereich auf dedizierte 6509-Switches mit WISM-Modulen abstützt, mit derzeit ca. 450 APs im Einsatz. 802.11n-fähige APs werden erst seit kurzem eingesetzt. Als Authentifizierungsverfahren für den Zugang zum WLAN kommt 802.1X zu Einsatz. Für die Verschlüsselung werden WPA und WPA2 eingesetzt. Für Gäste ist der Netzzugang mit eduroam/DFN-Roaming möglich.

Die WLAN-Versorgung soll noch wesentlich ausgebaut werden. Eine Umfrage unter den Nutzern in 2009 hat gezeigt, dass das WLAN eines der am stärksten nachgefragten Angebote des ZIV ist. Es ist langfristig geplant, eine WLAN-Vollversorgung mit 802.11n zumindest für Datenkommunikation (mit final ca. 3.000 APs) zu realisieren. In einigen Bereichen soll die WLAN-Abdeckung auch für VoIP over WLAN und evtl. für Location und Tracking ausgelegt werden. Aus Kostengründen soll von der bisherigen 1:1-Redundanz bei den zentralen WLAN-Switches auf eine 2:1-Redundanz umgestellt werden. Zusätzlich ist die Beschaffung von entsprechender WLAN-Messtechnik begleitend ebenso erforderlich wie die Schaffung von NAT- und Web-Proxy-Lösungen.

4.2.6 Erschließung von Studierendenwohnheimen

Die ca. 20 Studierendenwohnheime in Münster sind an das Glasfasernetz der WWU angeschlossen. Von hier erfolgt ein authentifizierter Zugang in das Netz der WWU. In den einzelnen Wohnheimen liegen unterschiedliche Netzinfrastrukturen vor. Im Falle einer LAN-Verkabelung erfolgt der Zugang mittels VPN-Technologie (PPTP). Bei einer DSL-Infrastruktur wird der Zugang mit PPPoE realisiert. In den ca. 15 Wohnheimen des Studentenwerks Münster existiert eine DSL-Versorgung der T-Systems. In Zusammenarbeit mit dem ZIV (sog. *Teleport-Projekt)* ist hier ein Netzzugang realisiert. Das ZIV betreibt dabei die für die Aggregation und Authentifizierung der Nutzer notwendigen Router.

4.2.7 Data Center

Derzeit existieren an der WWU zwei zentrale Server-Standorte. Es wird von einem Trend zur stärkeren Zentralisierung bei den Servern und dem Server-based Computing

sowie einer Konvergenz von LAN und SAN (Data-Center-Ethernet, FCoE, ...) ausgegangen. Eine Kapazitätserweiterung durch einen dritten Standort ist daher in Planung. Spezielle Data Center Switches mit hoher 10GE-Portdichte werden noch nicht eingesetzt. Zukünftig sollen diese Switches angeschafft und an den Midrange-Bereich angebunden werden. Die Aufteilung der Funktionen auf die Data Center soll so erfolgen, dass das IP-Routing zu den Data Centern auf den Midrange-Switches (d.h. ohne Belastung der Core-Switches) erfolgt. Die Abb. 1 verdeutlicht die Planungen. Die drei Data Center werden wie dargestellt untereinander und an jeweils 2 Midrange-Switches angebunden. Das Redundanzkonzept sieht vor, dass auch im K-Fall Data Center-Services zur Verfügung stehen. Hierfür wird einem Paar von Midrange-Switches ein Data Center für die Layer3-Anindung zugeordnet.

4.3 Konzept der netzseitigen IT-Sicherheitsmaßnahmen

4.3.1 Grundstrukturen für netzseitige Sicherheitsmaßnahmen

Netzseitige Maßnahmen erlauben das Gefährdungspotential für Netzbereiche auch dann zu begrenzen, wenn lokale, organisatorische und sonstige Maßnahmen nicht ausreichend umgesetzt werden konnten. Hierfür erfolgt eine Strukturierung des Netzes in sog. *Netzzonen* (VLANs) für Endsysteme mit identischem Sicherheitsbedarf. Netzzonen sind spezifische Sicherheitsfunktionen zugeordnet. Die Sicherheitsfunktionen sind in das Netz eingebettet; d.h. auf Netzkomponenten realisiert. Durch die Hierarchisierung von Netzzonen können Gesamtheiten von Netzzonen gegenüber anderen Netzzonen sicherheitstechnisch definiert werden. Netzseitig werden folgende Sicherheitsfunktionen eingesetzt:

- Stateless Packet Screening auf Layer-3 (IP-ACLs)
- Firewall-Funktionalität (Stateful Packet Screening)
- Intrusion-Prevention-Systeme (IPS)
- VPN-Technologie (insb. für den Zugang zu einer bestimmten Netzzone)
- Application Gateways oder Application Proxies
- *Bypassing:* Bypassing erlaubt den Einsatz von Sicherheitsfunktionen, wenn Anwendungen hohen Durchsatz erfordern. Beim Bypassing wird mittels Policy Based Routing bestimmter Datenverkehr an den durchsatzbeschränkenden Sicherheitsfunktionen vorbei gelenkt.

4.3.2 Realisierung durch Virtualisierung und mandantenfähige Administration

Netzstrukturen und funktionale Instanzen werden nicht 1:1 physisch bzw. physikalisch auf das Netzinventar abgebildet, sondern weitestgehend in virtualisierter Form realisiert.

- Mit *VLANs* können Netzzonen gebildet werden.

- Durch *Virtualisierung von IP-Routern* können flexibel Netztopologien aufgebaut werden. Zusammen mit der VLAN-Technologie kann im Grundsatz jede beliebige IP-Topologie mit den gewünschten hierarchischen Sicherheitszonen aufgebaut werden.
- Durch die *Virtualisierung von Firewall-* und *Intrusion-Prevention-Funktionalität* können Instanzen solcher Sicherheitselemente an beliebiger Stelle in das Netz eingebettet werden.
- *VPN-Technologie* erlaubt die Ausdehnung einer Netzzone auf externe Sites oder Clients

Im Konzept werden zentrale und dezentrale IT-Verantwortlichkeiten abgebildet. Folgende Funktionalitäten sind daher für eine effiziente Administration der Sicherheitsfunktionen erforderlich:

- *Mandantenfähigkeit* für Einsicht und Konfiguration der Sicherheitsfunktionen durch Netzzonen-Verantwortliche
- *Rahmenkonfigurationsmöglichkeiten und andere Generalfunktionen* für die Vorgabe von Muster-, Standard- und Mindestkonfigurationen

Beim eingesetzten IPS-Produkt sind diese Funktionalitäten gegeben. Für die besprochenen Netzbasisfunktionen VLANs, Virtuelle Router mit den Stateless-Packet-Screening-Funktionen und Virtuelle Firewalls ist die Mandantenfähigkeit bei den eingesetzten Produkten nicht verfügbar. Hier soll die Self-Care-Funktionalität der eigenentwickelten Netzdatenbank (*LANbase*) des ZIV im Rahmen einer Netzzonenverwaltung ausgebaut und mit Geräte-Steuerungsmechanismen verbunden werden.

4.3.3 Planungen bei den netzseitigen IT-Sicherheitsmaßnahmen

Bei den installierten Sicherheitsfunktionen muss zukünftig durchgängig ein Upgrade auf 10GE-Technologie durchgeführt werden. Als zusätzliche Sicherheitsfunktionalität soll eine Content-Filtering/Web-Proxy-Lösung realisiert werden. Der authentifizierte Netzzugang mittels 802.1X soll großflächig zum Einsatz kommen. Im Bereich der Statusüberwachung von Endsystemen (Policy Enforcement, NAC: Network Admission Control) gibt es derzeit noch keine Realisierung. Es ist beabsichtigt, auch diese Funktionalität zukünftig zu implementieren.

4.3.4 Organisatorische Maßnahmen im Rahmen der Netzsicherheit

Die Erarbeitung von Netzstrukturierungs-Konzepten (Definition von Netzzonen) durch das ZIV gemeinsam mit den Nutzern ist ein wesentlicher organisatorischer Bestandteil der Netzsicherheit. Mit Hilfe des selbst entwickelten Werkzeugs ISidoR wurde ein Sicherheitsaudit gemäß BSI Grundschutz Richtlinien durchgeführt. Die Anfang 2009

durchgeführte Sicherheitsbegehung hatte wichtige Impulse gegeben und soll auch zukünftig in regelmäßigen Abständen wiederholt werden.

4.4 House-Keeping: USV-Versorgung, Klimatisierung

USV-Anlagen sind primär an Standorten eingesetzt, die eine strukturelle Bedeutung für das Netz haben. Es existieren drei große USV-Anlagen an zwei Hauptnetzstandorten und einem Serverstandort. Für die Standorte existiert jeweils eine Netzersatzanlage (NEA, Dieselpufferung). An einigen Midrange-Standorten existieren USV-Versorgungen, die erneuert werden müssen. An Standorten, an denen ein Stromausfall nur lokale Auswirkungen hat, ist in der Regel keine USV-Absicherung realisiert. Bei VoIP-Installationen in Gebäuden wird eine USV-Versorgung nicht in jedem Fall realisiert. Angestrebt wird, zumindest den Midrange- und Distribution-Bereich vollständig mit einer USV-Versorgung zu versehen. Weitere USV-Versorgungen einzelner Bereiche unterliegen einer Einzelfallentscheidung. Ein USV-Versorgungsgrad von ca. 30% wird angestrebt. Die Spannungsversorgung für VoIP-Telefone und WLAN-Access-Points erfolgt über Power over Ethernet (PoE). Die obigen Ausführungen zur USV-Versorgung gelten im Grundsatz auch für die Klimatisierung der LAN-Verteilerräume.

4.5 Mediennetze, AVM (Audiovisuelle Medien)

Alle installierten medientechnischen Anlagen sind mit LAN Anschlüssen ausgestattet worden. Somit ist gewährleistet, dass die zukünftige Vernetzung der medientechnischen Anlagen über das LAN möglich ist. Zentraler Zugriff auf die Anlagen (mittels eines aufzusetzenden Managementsystems) erlaubt die Überprüfung der Funktionen und der Verfügbarkeit der Anlagen. Im Zuge der in den vergangenen Jahren umgesetzten medientechnischen Konzepte ist in einigen Gebäuden die Möglichkeit der Übertragung von Veranstaltungen innerhalb des Gebäudes realisiert worden. Eine Abstützung der Übertragungen aus den einzelnen Hörsälen findet z.Zt. nicht standardmäßig über die LAN Infrastruktur statt. Das zukünftige Konzept für die Übertragung von Veranstaltungen beinhaltet als Basisinfrastruktur das lokale Netz der WWU. Encoder- und Decoder-Technologie werden hierfür in den einzelnen Gebäuden der WWU bereit zustellen sein.

4.6 Core Network Services

Folgende CNSs (Core Network Services) werden vom ZIV zentral für die WWU und das UKM betrieben: DNS, DHCP, WINS, RADIUS, NTP. Die für den Betrieb dieser Services notwendige Verwaltung von z.B. Rechnernamen, IP-Adressen und MAC-Adressen ist mit Hilfe der Netzwerkdatenbank *LANbase* (vgl. 6.1) vollständig zentralisiert. In LANbase sind u.a. umfassende IPAM-Funktionen (Internet Protocol Address Management) realisiert. Über eine Webschnittstelle (sog. *NIC_Online*) können die für Endsysteme technisch Verantwortlichen Änderungen weitgehend selbst vornehmen. Die Provisionierung des DNS-, DHCP- und WINS-Services erfolgt aus LANbase heraus. Beim zentralen DNS-Service ist dabei die Anbindung an die für den

Betrieb einer Microsoft Active Directory Infrastruktur notwendigen DNS-Funktionen gegeben. Der RADIUS-Service wird aus der zentralen Nutzerdatenbank provisioniert. Die Produktivsysteme aller oben genannten Services werden auf einer nicht virtualisierten Serverplattform betrieben. Dabei kommen Linux als Betriebssystemplattform und Open Source Software zum Einsatz. Da die CNSs (insb. der DNS-Service) für den Netzbetrieb von herausragender Bedeutung sind, soll eine eigene umfassende Überwachung (Verfügbarkeit, Datenaktualität, Datenkonsistenz) für der CNSs realisiert werden.

5 Konvergenz von Tele- und Datenkommunikation

5.1 Darstellung der TK-Infrastruktur

Der TK-Anlagenverbund besteht aus Sopho iS3000 Systemen des Hersteller NEC. 19 Primärmultiplexanschlüsse (PRI) an 6 Standorten und ein VoIP-Zugang über das DFN (X-WIN Anschluss) sind als Anschaltungen an das öffentliche Netz realisiert. Eine verstärkte Nutzung des X-WIN Anschlusses für VoIP ist geplant. Die hierfür erforderliche Absicherung durch einen redundanten X-WIN-Anschluss ist gegeben. Die Anzahl der PRI-Anschlüsse soll dadurch halbiert werden, was zu einer deutlichen Kostenreduzierung führt. Vertragspartner ist in beiden Fällen der DFN-Verein.

5.2 Personal

Anfang des Jahres 2008 wurde die Konvergenz von Tele- und Datenkommunikation an der WWU organisatorisch vollzogen. Der Bereich *Kommunikations- und Medientechnik* der Universitätsverwaltung wurde in das ZIV integriert (hausinterne Bezeichnung: *Fusion*). Die betroffenen Mitarbeiterinnen und Mitarbeiter sind zusammen mit Ihren Aufgaben, u.a. Bereitstellung von Telekommunikations- und Vermittlungs- und Auskunftsdiensten am Hochschulstandort Münster, sowie Bereitstellung von audiovisueller Medientechnik für die WWU, nun in der Abteilung Kommunikationssysteme des ZIV angesiedelt.

5.3 Gemeinsame Nutzung von Netzinfrastruktur und Werkzeugen

Bereits vor der Fusion gab es zwischen den zuvor organisatorisch getrennten Bereichen eine enge Zusammenarbeit. So wurde beispielsweise das LWL-Netz gemeinschaftlich genutzt. Auch die ersten VoIP-Installationen wurden bereits vor der Fusion gemeinsam vorangetrieben. Das im TK-Bereich genutzte hochpaarige Kupferkabelnetz ist Bestandteil des gemeinsamen Kommunikationsnetzes geworden und stellt eine beträchtliche Ressource dar. Der Einsatz von DSL-Technologie stellt eine Komplettierung der Datenübertragungstechnik des ZIV dar und schützt die bereits getätigten Investitionen in das Kupferkabelnetz der WWU. Die Netzdatenbank *LANbase* und das Trouble-Ticket-System (Eigenentwicklung *NOCase*) werden inzwischen gemeinschaftlich genutzt.

5.4 Planung der VoIP-Migration

An der WWU werden ca. 8.500 konventionelle Telefone betrieben, sodass die Migration zu VoIP in mehreren Schritten erfolgt. Die Serviceunterstützung der TK-Anlage ist durch den Hersteller bis 2017 gesichert. Dieser Zeitpunkt wird an der WWU für die vollständige Migration nach VoIP angestrebt. Der TK-Anlagenverbund wurde frühzeitig um VoIP-Technologie, nach SIP Standard der IETF, ergänzt. Diese frühzeitige Entscheidung stellt einen substantiellen Investitionsschutz dar. Alle wichtigen Leistungsmerkmale können in der gemischten Systemumgebung realisiert werden. Die Anschaltung weiterer Serverapplikationen an den Verbund geschieht unter der Maxime, dass offene Schnittstellen und standardisierte Protokolle vorrangig berücksichtigt werden. SIP-Standard konforme Endgeräte können prinzipiell unterstützt werden, was einen hohen Freiheitsgrad bei der Beschaffung und der Marktbeobachtung bedeutet, wobei jedoch aufgrund der Logistik, der notwendigen Vorhaltung von Endgeräten, sowie insbesondere der Unterstützung von Leistungsmerkmalen, die über den SIP Standard hinausgehen, vorrangig Endgeräte des Hersteller Polycom eingesetzt werden. Zusammen mit der VoIP-Migration soll in 2011 eine flächendeckende Bereitstellung von Unified Communications-Services realisiert sein.

Die Migrationsstrategie sieht vor, dass bei Neubauten oder Sanierungen VoIP als Technik eingeführt wird. Bei einer Teilsanierung wird möglichst auch eine VoIP-Umstellung der nicht sanierten Bereiche realisiert. LAN-Netzkomponenten sollen über redundante Netzteile, Priorisierungsmöglichkeiten und PoE-Funktionalität für die Versorgung der Telefone verfügen. Die Anbindung der VoIP-Telefone an die TK-Units erfolgt mittels des SIP-Protokolls über ISG-Baugruppen (In System Gateway). VoIP-Telefone werden dabei wie fest angeschlossene, registrierte Rechner betrieben. Um eine angemessene Dienstgüte der VoIP-Kommunikation zu realisieren, wurde bislang eine Überprovisionierung ohne Qualitätseinbußen vorgenommen. Zukünftig könnte eine Priorisierung der VoIP-Kommunikation notwendig sein. Ggf. soll dann eine datenbankgestützte Konfiguration dieser Funktionen realisiert werden.

6 Betriebs- und Managementkonzept

6.1 Administration, Dokumentation

Als zentrale Servicestelle für alle Aspekte der Netzdokumentation und -administration ist ein NIC (Network Information Center) eingerichtet. Das Hauptwerkzeug für die Netzdokumentation und -administration ist die auf einer Oracle-Datenbank basierende, langjährige Eigenentwicklung *LANbase*. *LANbase* wird dabei nicht nur zur Dokumentation, sondern auch für ein breites Spektrum an administrativen Aufgaben verwendet. LANbase ist gekoppelt an das Produkt EMS (Enterprise Management Suite) der Firma 3Com. EMS ist ein Workflow Automation Tool (z.B. für Konfigurations- und Change-Management von Netzkomponenten). Mit LANbase steht eine Fülle von Funktionalitäten einer CMDB (Configuration Management Database) nach ITIL zur Verfügung. In LANbase ist u.a. die einheitliche Verwaltung und Administration einer

Vielzahl von netztechnischen Objekten, Systemen und Vorgängen realisiert. Auszüge aus dem LANbase-Datenbestand stehen mandantenfähig den Systemverantwortlichen der WWU als User-Self-Care-Portal *NIC_online* zur Verfügung.

Mit steigender Ausdehnung und Komplexität des Netzwerkes werden elaborierte Werkzeuge zum Betrieb immer wichtiger. Da eine zu LANbase funktional vergleichbare kommerzielle Lösung nicht bekannt ist, wird die bewährte Weiterwicklung an *LANbase* als effektive und kosteneffiziente Notwendigkeit gesehen. Es sollen hierbei insbesondere die bereits eingeführten mandantenfähigen User-Self-Care-Funktionen noch weiter ausgebaut werden.

Als weiteres Netzdokumentationswerkzeug existiert die auf AutoCad basierende Eigenentwicklung *LANcad*. Mit LANcad werden Grundrisspläne verwaltet und die topografische Dokumentation von Kabeln, Kabeltrassen, Anschlussdosen, etc. durchgeführt. Für LWL-Strukturpläne wird darüber hinaus noch VISIO verwendet.

6.2 Betrieb

Die weitgehende Redundanz im Netzdesign ist eine der wichtigsten Maßnahmen zur Sicherstellung eines störungsfreien Netzbetriebs. Für alle wichtigen Geräte bestehen Wartungsverträge, die einen Geräteaustauschservice („Next Business Day“ oder 4h) bei Defekt, Hotline-Support und vor Ort-Support bei technischen Problemen und den Zugriff auf die neuesten Softwareversionen für die Geräte beinhalten. Darüber hinaus wird für alle wichtigen Netzkomponenten eine eigene Ersatzteilhaltung durchgeführt. In Fällen in denen eine Ersatzteilhaltung aufgrund der Kosten unangemessen ist, wird durch Wartungsverträge ein Hardwaretauch innerhalb 4 Stunden gewährleistet. Damit kann bei einem Geräteausfall schnellstmöglich ein Austausch vorgenommen werden. Die Ersatzgeräte werden außerdem für Testzwecke verwendet. Als wesentliche Betriebswerkzeuge werden eingesetzt:

- LANbase (CMDB, siehe 6.1)
- Konfigurations- und Änderungsmanagement: 3Com EMS
- Netzüberwachung: CA SPECTRUM
- Trouble Ticket-System: in LANbase integrierte Eigenentwicklung NOCase
- Diverse Test- und Messgeräte, sowie Protokollanalysatoren

Als zentrale Einheit für den Betrieb des Datennetzes ist ein Network Operating Center (NOC) eingerichtet, in dem u.a. folgende Aufgaben angesiedelt sind: Annahme von Störungsmeldungen, Netzüberwachung und Entstörung, Konfigurations- und Änderungsmanagement. Um für den NOC-Service einen möglichst hohen Service-Level zu gewährleisten, sind eine Reihe von Maßnahmen umgesetzt worden:

- Erreichbarkeit über Telefon-Hotline, E-Mail, Web-Formular

- Personelle Zuordnung per Dienstplan für einen Präsenzdienst mit garantierter Erreichbarkeit während der Service-Zeiten: Mo – Fr, 8:00 – 16:30 Uhr für die Störungsbehebung
- separate Räumlichkeiten für Präsenzdienst
- außerhalb der o.g. Zeiten doppelte Rufbereitschaft (First- und Second-Level-Support)

Im Jahr 2009 wurden hier 6.327 Trouble Tickets (WWU und UKM) bearbeitet. Dabei handelte es sich zu 33,2% um Störungen, zu 54,2% um Änderungswünsche und zu 6,3% um Beratungsfälle.

Im TK-Bereich besteht ein Serviceunterstützungsvertrag, über den im Bedarfsfall Zugriff auf den Support des Herstellers besteht. In den Bereichen TK und AVM ist die Erreichbarkeit über Telefon-Hotline, E-Mail und Online-Formulare werktags in der Zeit von 7:30-16:00 Uhr gegeben. Außerhalb dieser Zeiten besteht eine Rufbereitschaft für die Beseitigung von Störungen über die TK-Mitarbeiter. Für das Management der TK-Infrastruktur (inkl. VoIP) soll eine Lösung mit umfangreichen User-Self-Care-Funktionen implementiert werden.

6.3 Netzüberwachung

Für die Überwachung sämtlicher IP-basierten Komponenten des Kommunikationsnetzes wird das Produkt CA SPECTRUM eingesetzt. Dies umfasst derzeit die eigentlichen Netzwerkkomponenten (z.B. Router, Switches, ...), Infrastrukturkomponenten (z.B. USVs) und die CNS-Server. SPECTRUM wird routinemäßig im Rahmen der Betriebsüberwachung durch das NOC genutzt. Eine Anbindung an das eingesetzte Trouble-Ticket-System NOCase ist realisiert. Um ein zeitnahes Einpflegen von Änderungen im Netz zu gewährleisten ist die regelmäßige Pflege des mit SPECTRUM zu überwachenden Gerätebestandes in die internen Betriebsabläufe integriert. Die zu überwachenden Technologien sollen stetig erweitern werden (z.B. Routing-Protokolle, Virtualisierung). Außerdem ist ein umfassendes Netzreporting für ein effektives proaktives Ressourcenmanagement geplant. Im ZIV wird begonnen mit den nutzenden Einrichtungen (UKM, Fachbereiche, Verwaltung) verbindliche Dienstqualitäten und -quantitäten zu verabreden und somit die Verlässlichkeit des Netzbetriebes zu regeln und für den Nutzer transparent zu machen. Daher ist auch ein Kundenportal für den Zugang zu Netzwerküberwachungsinformationen (Service-Überwachung) in der Planung.

Identity Management

Integration bestehender IP-basierter Autorisierung und Abrechnung in Shibboleth-basierte Föderationen

Sebastian Rieger

Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen (GWDG)
Am Fassberg
37075 Göttingen
sebastian.rieger@gwdg.de

Abstract: Insbesondere im wissenschaftlichen Umfeld stellen Verlage und Bibliotheken in den letzten Jahren vermehrt Ihre Zugriffskontrolle für die von Ihnen bereitgestellten Ressourcen von IP-basierten auf föderative Verfahren um. Ausgehend von Entwicklungen im Rahmen des Internet2 in den USA hat sich für föderative Authentifizierungs- und Autorisierungsverfahren im wissenschaftlichen Umfeld das auf der Security Assertion Markup Language (SAML) basierende Shibboleth etabliert. Shibboleth ermöglicht durch den föderativen Ansatz ein Single Sign-On über unterschiedliche Web-Ressourcen innerhalb einer Föderation. Allerdings umfasst weder Shibboleth noch der SAML-Standard explizite Funktionen für die Unterstützung des Accounting bzw. der Abrechnung von Zugriffen. Eine differenzierte Abrechnung ist jedoch vor Allem dann erforderlich, wenn innerhalb einer Föderation unterschiedliche Organisationen existieren (z.B. unterschiedliche Einrichtungen, die die Leistungen einer gemeinsamen Bibliothek in Anspruch nehmen). Die folgenden Abschnitte stellen eine Lösung vor, die im Rahmen der Realisierung einer Shibboleth Föderation für die 80 Institute der Max-Planck-Gesellschaft (MPG-AAI) in Bezug auf die Integration von IP-basierten und föderativen Abrechnungs- und Autorisierungsverfahren erstellt wurde. Durch die vorgestellte Implementierung wird die Integration von Verlagen, die nach wie vor eine IP-basierte Autorisierung durchführen, in die Föderation möglich ohne dabei die differenzierte Abrechnung der einzelnen Institute der Max-Planck-Gesellschaft einzuschränken. Dies ermöglicht eine sanfte Migration hin zu föderativen Authentifizierungs- und Autorisierungsverfahren innerhalb der Max-Planck-Gesellschaft.

1 Zugriffsschutz auf Web-Ressourcen bei Verlagen

In der Vergangenheit wurde der Zugriff auf Web-Ressourcen wissenschaftlicher Verlage insbesondere durch die Prüfung der IP-Adresse des Clients von dem aus der Zugriff erfolgt geschützt [Mike04]. Benutzer, die über eine vom jeweiligen Verlag akzeptierte IP-Adresse verfügten wurden durch diese Adresse gleichermaßen authentifiziert und autorisiert. Um die Authentifizierung und Autorisierung an unterschiedlichen Web-Seiten unabhängig von der IP-Adresse einheitlich zu realisieren, wurden in den letzten Jahren unterschiedliche Verfahren entwickelt. Sie lassen sich in föderative und benutzerzentrierte Verfahren einteilen [Rieg09].

Föderative Verfahren basierend dabei in der Regel auf dem Security Assertion Markup Language (SAML) Standard [SAML]. Eine insbesondere in wissenschaftlichen IT-Infrastrukturen weit verbreitete Implementierung des SAML-Standards bildet Shibboleth [MCHK04]. Wesentlicher Treiber hinter der Einführung von Shibboleth sind und waren dabei auch Bibliotheken und Verlage, die Ihren Nutzern einen Zugriff unabhängig von deren aktueller IP-Adresse erlauben wollten, ohne dabei für jeden Verlag eine separate Anmeldung bzw. Benutzerkonten zu benötigen [vasc]. Die Verwendung separater Benutzerkonten für die Benutzer bei den Verlagen ist nicht zuletzt aufgrund der hohen Fluktuation in wissenschaftlichen Umgebungen nicht realisierbar [RiNe07]. Eine geeignete Lösung bieten dezentrale Authentifizierungsverfahren, wie z.B. die föderative Authentifizierung, bei denen direkt die Benutzerkonten der Heimatinstitute der Anwender verwendet werden können. Obwohl einige Verlage bereits auf föderative Authentifizierungsverfahren umgestellt haben, verwendet die Mehrzahl weiterhin eine IP-Adressbasierte Zugangskontrolle [Mike04]. Dies ist vorrangig in der Komplexität von föderativen im Vergleich zu IP-basierten Verfahren begründet. Um den Benutzern innerhalb einer Föderation auch diese Anbieter bzw. Verlage zugänglich zu machen, wurden unterschiedliche Proxy Lösungen für Bibliotheken (wie z.B. der OCLC EZproxy [EZp]) um föderative Authentifizierung und Autorisierung erweitert. Alle Benutzer des Proxy erhalten hierbei innerhalb der Föderation dessen IP-Adresse als Quell-Adresse beim Zugriff auf die Verlage. Mit dieser einzelnen IP-Adresse ist auf der Seite der Verlage keine differenzierte Autorisierung und Abrechnung, z.B. von unterschiedlichen Instituten, die den Proxy verwenden, möglich. Dieses Paper beschreibt eine Lösung, die für die 80 Institute der Max-Planck-Gesellschaft innerhalb von deren MPG-AAI Föderation [MPAAI] realisiert wurde, um die genannten Einschränkungen zu adressieren, und eine institutsbezogene Autorisierung und Abrechnung zu erlauben. Die Grundlage für den Zugriff auf die Ressourcen liefern hierbei Verträge zwischen den Verlagen und der Max-Planck Digital Library (MPDL). Gemeinsam mit dem Rechenzentrum Garching (RZG) betreibt die Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen (GWDG) einen Proxy, der die Benutzer der MPG-AAI entsprechend ihrer Institute auf separate IP-Adressen abbildet und so der MPDL eine differenzierte Abrechnung sowie die Erhebung institutsbezogener Nutzungsstatistiken erlaubt.

1.1 IP-basierte Zugriffskontrolle für den Zugriff auf Web-Ressourcen

Anhand der Kontrolle der Quell-IP-Adresse, die der Web-Client (bzw. Web-Browser) des Anwenders verwendet, lässt sich eine einfache Zugriffskontrolle realisieren. Wissenschaftliche Einrichtungen verfügen in der Regel über einen gesonderten IP-Adressbereich (bzw. IP Subnetz), anhand dessen alle Benutzer des Instituts eindeutig identifiziert werden können. Die Autorisierung der Zugriffe sowie deren Abrechnung kann daher auf der Seite der Anbieter anhand der Quell-IP-Adresse durchgeführt werden. Abbildung 1 zeigt ein Beispiel für diese konventionelle Differenzierung von Zugriffen unterschiedlicher Institutionen auf Web-Ressourcen, die derzeit noch häufig von Bibliotheken und Verlagen verwendet wird [Eggl08]. Hierbei greift Benutzer i1.b1, der Angehöriger des Instituts i1 ist, welches das IP-Subnetz 192.168.0/24 verwendet (im Rahmen dieses Papers werden private Internet-Adressen für die Beispiele verwendet), auf eine Web-Ressource, die vom Verlag v1 angeboten wird, zu.

Der Verlag verwendet die Quell-IP-Adresse des HTTP-Requests, um zu entscheiden, ob der Benutzer für den Zugriff autorisiert ist. Üblicherweise werden hierfür die IP-Adressbereiche der aus Sicht des Verlags zugriffsberechtigten Institutionen beim Anbieter in entsprechenden Tabellen hinterlegt. Erfolgt danach ein Zugriff des Benutzers i2.b1, welcher dem Institut i2 angehört, auf Ressourcen des Verlags v1, kann dieser aufgrund der Quell-IP-Adresse 192.168.1.11 dem Institut i2 zugeordnet und so die unterschiedlichen Institute der beiden Benutzer i1.b1 und i2.b1 differenziert werden. So kann der Verlag v2 z.B. anhand der Quell-IP-Adresse Benutzer des Instituts i1 zulassen und Zugriffe von Benutzern des Instituts i2 verweigern.

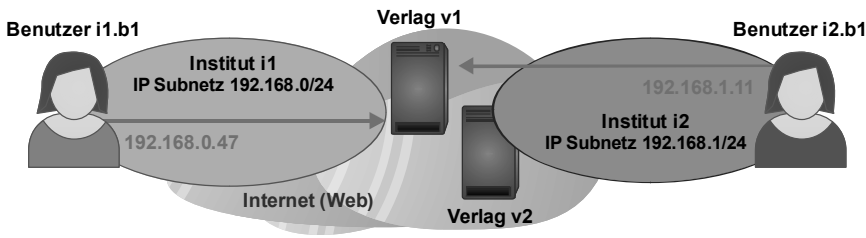


Abbildung 1: Differenzierung der Quell-IP-Adressen beim Zugriff auf Web-Ressourcen.

Während die in Abbildung 1 gezeigte Zugriffskontrolle für die Verlage sehr einfach zu implementieren ist, birgt das Verfahren einige Nachteile. Zum Einen können Quell-IP-Adressen gefälscht bzw. durch zusätzliche Gateways / Proxy-Lösungen etc. manipuliert werden (z.B. IP Spoofing). Durch die Auswertung der Quell-IP-Adresse kann somit keine Authentifizierung gewährleistet werden. Zum Anderen müssen die Benutzer bzw. deren Clients sich innerhalb des Subnetzes ihres jeweiligen Instituts befinden, damit ein Zugriff auf die Verlage erfolgen kann. Häufig werden Lösungen wie Proxy-Server oder VPN, die den Benutzern auch einen mobilen Zugriff auf das Subnetz ihres Instituts erlauben würden, in den Verträgen von den Verlagen ausgeschlossen, sofern keine zusätzlichen Maßnahmen für die Gewährleistung der Authentizität der Benutzer ergriffen werden. Diese Einschränkungen stehen den Anforderungen nach Mobilität innerhalb von wissenschaftlichen IT-Infrastrukturen z.B. durch deren räumliche Verteilung (vgl. virtuelle Organisationen oder weltweit kooperierende Forschungsprojekte) entgegen [RiNe07]. Ein zusätzliches Problem entsteht, wenn unterschiedliche Institutionen ein gemeinsames Subnetz verwenden (z.B. bedingt durch eine Kooperation in Bezug auf die Internet-Anbindung zwischen Universitäten und Forschungsinstituten eines Standorts).

1.2 Föderative Authentifizierung und Autorisierung

Im vorherigen Abschnitt wurden unterschiedliche Nachteile von IP-basierten Zugriffskontrollverfahren beschrieben. Um diese Probleme zu adressieren wurden in den letzten Jahren dezentrale Authentifizierungs- und Autorisierungsmechanismen eingeführt. Hierbei kann zwischen föderativem und benutzerzentriertem Identity Management unterschieden werden [Rieg09]. Einige Verlage haben, wie im Abschnitt 1 beschrieben, ihre Zugriffskontrolle bereits auf föderative Authentifizierungsverfahren (z.B. das SAML-basierte Shibboleth) umgestellt.

Um föderative Authentifizierungsverfahren zu unterstützen, implementieren die Verlage einen sog. Service Provider (SP) [Morg04] und schließen sich damit einer oder mehreren Föderationen an, die die Benutzer bzw. Kunden der Verlage enthalten. Auf der anderen Seite betreiben die Institute hierfür ihrerseits sog. Identity Provider (IdP) [Morg04], die ihren Benutzern den Zugriff auf SPs innerhalb der Föderation erlauben. Beispielsweise betreibt der DFN-Verein eine Föderation (DFN-AAI), der sich bereits einige Verlage angeschlossen haben [DV], und an die auch die MPG-AAI angebunden ist.

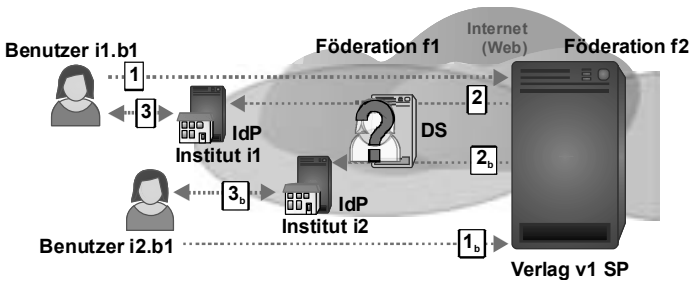


Abbildung 2: Zugriff auf Verlage innerhalb einer Föderation aus unterschiedlichen Instituten.

Abbildung 2 zeigt den Verlag v1, der sich den Föderationen f1 und f2 als Service Provider (SP) angeschlossen hat. In dem oben gezeigten Beispiel enthält die Föderation f1 zusätzlich die Institute i1 und i2 bzw. deren Benutzer (z.B. i1.b1 und i2.b1). Greift der Benutzer i1.b1 auf vom Verlag v1 angebotene Ressourcen zu (1), so wird er von dessen SP zum Discovery Service (DS) der Föderation f1 umgeleitet (2), der die Lokalisierung des Heimatinstituts übernimmt. Nachdem der Benutzer sein Heimatinstitut am DS ausgewählt hat, leitet ihn dieser an dessen IdP weiter [Morg04]. Anschließend erfolgt die Anmeldung des Benutzers am IdP (3). Nach erfolgreicher Authentifizierung erstellt der IdP ein digital signiertes Ticket (sog. Assertion), mit dem er den Benutzer an den SP des Verlags v1 zu der ursprünglich ausgewählten Ressource weiterleitet. Zusammen mit der Assertion kann der IdP dem SP hierbei Attribute übermitteln, die für die Autorisierung verwendet werden. Beispielsweise kann eines dieser Attribute verwendet werden, um einen eindeutigen Bezeichner für das Heimatinstitut des Benutzers zu übermitteln. Der SP ist dann anhand dieses Attributs in der Lage die Institute zu differenzieren und z.B. spezielle Ressourcen nur einem bestimmten Institut anzubieten. Durch die Verwendung föderativer Authentifizierungs- und Autorisierungsverfahren kann der Zugriff auf die Verlage unabhängig von der Quell-IP-Adresse des Web-Clients erfolgen, den der Benutzer aktuell verwendet. Damit adressieren föderative Verfahren ein zentrales Problem der in Abschnitt 1.1 dargestellten IP-basierten Zugriffskontrollverfahren, ohne zusätzliche Benutzerkonten oder deren Synchronisation über die Verlage hinweg zu erfordern. Durch den SAML-Standard werden zusätzlich unterschiedliche Implementierungen bzw. Software-Lösungen auf der Seite der Verlage ermöglicht. Allerdings basiert die Zugriffskontrolle bei der Mehrzahl der Verlage, wie im vorherigen Abschnitt geschildert, noch auf der Auswertung der Quell-IP-Adresse. Eine einheitliche föderative Authentifizierung und Autorisierung, unabhängig von der Quell-IP-Adresse der Benutzer, kann somit derzeit für wissenschaftliche IT-Infrastrukturen nicht realisiert werden. Ein weiteres Problem bildet die fehlende Standardisierung von Attributwerten in Föderationen.

Während z.B. in der eduPerson sowie der dfnEduPerson [DEP] feste Schemata für die Definition der Attribute existieren, können IdP und SP unabhängig davon unterschiedliche Attributnamen und insbesondere Attributwerte z.B. für die Differenzierung unterschiedlicher Institute der Benutzer verwenden.

1.3 Accounting

Sowohl Shibboleth als auch der zugrundeliegende SAML-Standard wurden für die Vereinheitlichung der Authentifizierung und Autorisierung nicht jedoch der Abbrechnung (Accounting) entwickelt. Die fehlende Standardisierung von Attributen und Attributwerten für das Accounting führt auf der einen Seite zu Problemen bei den Verlagen, wenn die IdPs von deren Kunden jeweils unterschiedliche Attribute bzw. Attributwerte für die Abrechnung an die Verlage übertragen. Auf der anderen Seite ist es auch für die Institute aufwändig für einzelne Verlage unterschiedliche Attribute für die Abrechnung (z.B. eine eindeutige Kennzeichnung des Instituts) zu konfigurieren und zu verwenden. Die geschilderten Nachteile gelten insbesondere für Bibliotheken, die Nutzern unterschiedlicher Einrichtungen (z.B. bedingt durch die Angliederung an Universitäten und Forschungsinstituten) Zugang zu Diensten bzw. Verlagen in einer Föderation anbieten wollen. Hierbei müssen die Bibliotheken die Nutzung durch die jeweilige Einrichtung getrennt abrechnen. Häufig werden beispielsweise Nutzungsstatistiken erstellt, die der Bibliothek neben statistischen Analysen auch ermöglichen, Zugriffe auf Web-Ressourcen für einzelne Einrichtungen gesondert in Rechnung zu stellen. Zusätzlich können Vorgaben aus den Verträgen zwischen Bibliotheken und Verlagen für die getrennte Erfassung der Zugriffe einzelner Einrichtungen existieren.

Um differenzierte Nutzungsstatistiken für die angebundenen Einrichtungen zu erstellen, sind die Bibliotheken dabei auf die Übermittlung von Zugriffszahlen durch die Verlage angewiesen. Die Bibliotheken können dann als Abrechnungsstelle zwischen Verlagen und Benutzern agieren. Da für föderative Authentifizierungsverfahren keine standardisierten Accounting-Verfahren existieren, verwenden einige Verlage proprietäre Lösungen für die Übermittlung der Zugriffszahlen an die Bibliotheken. Andere verwenden weiterhin eine IP-basierte Abrechnung, die anhand der Quell-IP-Adresse des Benutzers ermittelt werden. Diese sind jedoch erneut ungeeignet, sobald die Benutzer z.B. mobil aus unterschiedlichen IP-Subnetzen Zugriff auf die Web-Ressourcen der Verlage erhalten sollen. Bibliotheken und angebundene Einrichtungen fordern daher eine benutzerbezogene Abrechnung unabhängig von der aktuellen IP-Adresse des Web-Clients.

2 Verwendung von Web-Proxy Lösungen in Föderationen

Wie im Abschnitt 1.2 erläutert, wird die IP-basierte Zugriffskontrolle nicht zuletzt aufgrund der geringeren Komplexität in Bezug auf die Implementierung nach wie vor von einer Vielzahl von Verlagen verwendet. Um Benutzern innerhalb einer Föderation Zugriff auf diese Verlage unabhängig von deren aktueller IP-Adresse zu ermöglichen, wurden verschiedene Proxy-Lösungen entwickelt. Innerhalb der Max-Planck-Gesellschaft wird hierfür der OCLC EZproxy [EZp] verwendet.

Die Abbildung 3 zeigt die Verwendung des Proxy-Servers für Verlage, deren Zugriffskontrolle nach wie vor auf der Quell-IP-Adresse des zugreifenden Web-Clients basiert, innerhalb einer Föderation.

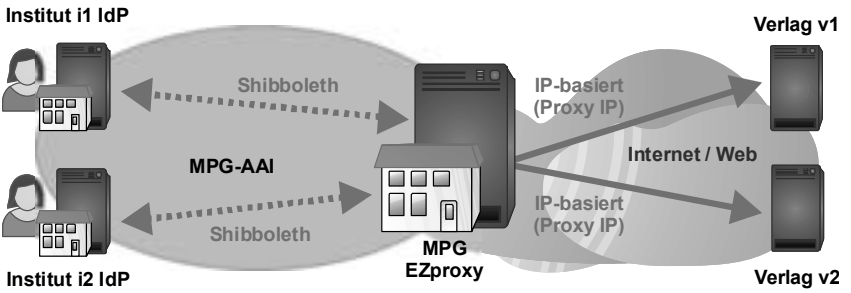


Abbildung 3: Einsatz eines Proxy-Servers für den Zugriff auf Verlage in einer Föderation

Die Abbildung zeigt einen Ausschnitt der MPG-AAI Föderation der Max-Planck Gesellschaft. In dem gezeigten Beispiel betreiben die Institute i1 und i2 für die Authentifizierung und Autorisierung Ihrer Benutzer einen Shibboleth IdP innerhalb der Föderation. Die Benutzer können sich an dem Web-Proxy „MPG EZproxy“ über die IdPs ihrer Institute authentifizieren und nach erfolgreicher Autorisierung auf die Ressourcen der Verlage v1 und v2 zugreifen. Der EZproxy bildet hierbei die Funktion eines Reverse Proxy für die Web-Ressourcen der Verlage. Benutzer können z.B. über die Adresse http://verlag-v1.proxy.aai.mpg.de auf den Verlag v1 zugreifen. Hierbei leitet der Proxy die Anfrage unter Verwendung seiner eigenen IP-Adresse als HTTP Request an den Verlag weiter. Der Verlag sendet anschließend die HTTP Response an den Proxy, der diese zurück an den Benutzer leitet. Da für die Autorisierung und das Accounting auf der Seite der Verlage die Quell-IP-Adresse des Proxy ausgewertet wird, können die Benutzer unabhängig von Ihrer aktuellen IP-Adresse Zugriff auf die bereitgestellten Ressourcen nehmen. Außerdem können die Benutzer alle Dienste der Föderation, z.B. Verlage die bereits eine föderative Authentifizierung unterstützen sowie den EZproxy, ohne separate Anmeldung nutzen. Durch die Authentifizierung und Autorisierung am EZproxy erfüllt dieses Single Sign-On auch die Anforderungen der Verlage in Bezug auf den Schutz der Ressourcen. Häufig schließt dies auch zusätzliche Anforderungen, wie z.B. maximale Gültigkeitszeiträume für Benutzer-Accounts bzw. eine zeitnahe Sperrung von Benutzer-Accounts, mit ein, die innerhalb der Policy der Föderation für alle Teilnehmer verbindlich vorgegeben werden. Die skizzierte Lösung erlaubt eine sanfte Migration zu föderativen Authentifizierungsverfahren, ohne den Benutzern den Zugriff auf Verlage, deren Zugriffskontrolle noch auf der Auswertung der Quell-IP-Adresse basiert, außerhalb des IP-Subnetzes ihres Instituts zu verweigern.

2.1 Realisierung einer mandantenfähigen Web-Proxy-Lösung für Föderationen

Während die im vorherigen Abschnitt beschriebenen Reverse-Proxy Server das Problem der Integration von Verlagen mit IP-basierter Zugriffskontrolle in Föderationen lösen, erlauben sie jedoch keine differenzierte Abrechnung. Alle Benutzer erhalten beim Zugriff auf die an den Proxy angebundenen Verlage die gleiche IP-Adresse.

Auf der Seite der Verlage kann nur die IP-Adresse des Proxy Servers für die Autorisierung und Abrechnung verwendet werden. Existieren innerhalb einer Föderation unterschiedliche Einrichtungen, die den Proxy nutzen, wie z.B. unterschiedliche Forschungseinrichtungen und Universitäten innerhalb der DFN-AAI, so können auf der Seite der Verlage keine einrichtungsbezogenen Zugriffe erlaubt oder abgerechnet werden. Dies ist, wie bereits in Abschnitt 1.3 erläutert, inakzeptabel für Bibliotheken, die die Verrechnung ihrer Leistungen anhand von Nutzungsstatistiken einzelner angebundener Einrichtungen durchführen. Eine mögliche Lösung für die differenzierte Abrechnung einzelner Nutzer der im vorherigen Abschnitt beschriebenen Web-Proxy Server innerhalb einer Föderation könnte die Übermittlung der vom IdP an den Web-Proxy als SP übertragenen Attribute sein. Beispielsweise könnte ein Attribut für die Institutszugehörigkeit auf eine HTTP Header Variable abgebildet werden, die der Proxy in den Requests an die Verlage überträgt. Allerdings würde dieses Verfahren erneut eine Standardisierung der übermittelten Variablen über unterschiedliche Verlagen und Institute hinweg erfordern. Ebenfalls wären Anpassungen auf der Seite der Verlage für die Auswertung der Variablen erforderlich. Um unabhängig von der aktuellen IP-Adresse des Web-Clients der Benutzer einen Zugriff auf alle innerhalb der Max-Planck-Gesellschaft verwendeten Verlage zu erlauben, wurde die in Abbildung 3 vorgestellte Reverse Proxy-Lösung, wie in Abbildung 4 dargestellt, um einen zusätzlichen Forward Proxy erweitert.

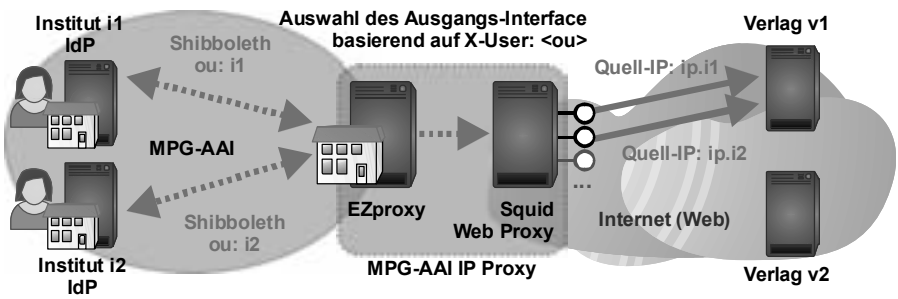


Abbildung 4: Kombination von Reverse und Forward Proxy für eine differenzierte Abrechnung und Autorisierung

Hierfür wurde ein zusätzlicher Squid Web Proxy [Squid] eingerichtet, über den der EZproxy seine ausgehenden HTTP Request sendet. Greift ein Benutzer auf eine Ressource des Verlags v1 (z.B. http://verlag-v1.proxy.aai.mpg.de) zu, so muss er sich erneut am EZproxy mittels Shibboleth Login am IdP seines Heimatinstituts authentifizieren. Dabei übermittelt jedes Institut eine eindeutige Institutskennung (Domain des Instituts z.B. institut-i1.mpg.de) in Form des OU Attributs. Der EZproxy kann dieses Attribut für die Autorisierung einzelner Institute an bestimmten Ressourcen verwenden. Für den Zugriff auf den Verlag sendet der EZproxy die Anfrage nach erfolgreicher Authentifizierung und Autorisierung an den Squid Proxy. Der EZproxy wurde hierbei erweitert, so dass der Header dieses HTTP Requests einen Parameter X-User mit der zuvor vom IdP erhaltenen Institutskennung (z.B. X-User: institut-i1.mpg.de) beinhaltet. Am Squid Proxy wurden für alle angeschlossenen Institute virtuelle Ausgangs-Interfaces mit separaten IP-Adressen eingerichtet.

Anhand des in den eingehenden HTTP Requests empfangenen X-User Headers wählt der Squid Proxy für jedes Institut ein individuelles Ausgangs-Interface und damit die Quell-IP-Adresse (tcp_outgoing_address) für den anschließenden HTTP Request an die Verlage. Verlage, die ihre Zugriffskontrolle und Abrechnung nach wie vor anhand der eingehenden IP-Adresse durchführen können so weiterhin, neben anderen die bereits föderative Verfahren einsetzen, verwendet werden. Die Max-Planck Digital Library erhält zusätzlich weiterhin institutsbasierte Nutzungsstatistiken von den Verlagen. Trotzdem können die die Benutzer unabhängig von deren aktueller IP-Adresse auch außerhalb des Subnetzes ihres Heimatinstituts alle für Ihre Forschung relevanten Verlage verwenden. Durch die Shibboleth-basierte Authentifizierung am EZproxy werden zusätzlich alle Sicherheits-anforderungen der Verlage erfüllt.

2.2 Fehlertoleranz und Lastverteilung über mehrere Standorte

Um einen ausfallsicheren und performanten Dienst der im vorherigen Abschnitt vorgestellten zentralen Proxy-Lösung für alle 80 Max-Planck-Institute zu realisieren, wurden mehrere „MPG-AAI IP Proxy“ Instanzen realisiert. Diese wurden über zwei Standorte, an denen Rechenzentren der Max-Planck-Gesellschaft existieren, verteilt. Ein Standort bildet die Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen (GWDG). Den zweiten bildet das Rechenzentrum Garching (RZG). Beide Rechenzentren betreiben jeweils zwei „MPG-AAI IP Proxy“ Instanzen. Für die Realisierung der Ausfallsicherheit über beide Standorte hinweg wurde ein nginx-basierter [nginx] Load Balancer (LB) als zusätzlicher Reverse Proxy vor den Instanzen der Rechenzentren installiert. Der nginx Server erhält dabei alle Zugriffe der Benutzer auf proxy.aai.mpg.de. Sobald eine „MPG-AAI IP Proxy“ Instanz nicht in der Lage ist, die eingehenden Requests der Benutzer zu beantworten, leitet der nginx Server diese an eine andere Instanz um. Zusätzlich werden die Requests über die beiden Instanzen am jeweiligen Standort verteilt und so eine Lastverteilung erzielt. Durch die Anmeldung am IdP können bei einem Ausfall einer Instanz alle Anfragen von zuvor angemeldeten Benutzern auf eine andere Instanz umgeleitet werden, ohne ein erneutes Login der Benutzer zu erfordern.

Da eine IP-Adresse nur einmalig im jeweiligen Subnetz vergeben werden kann, besitzen die teilnehmenden Institute an den Standorten jeweils zwei IP-Adressen, wie in Abbildung 5 gezeigt. Ohne diese zusätzliche IP-Adresse wäre an einem einzelnen Standort keine Lastverteilung realisierbar. Die Anfragen eines Instituts würden alle über die gleiche Ausgangs-IP-Adresse eines einzelnen Squid Proxy laufen. Greift beispielsweise ein Benutzer des Instituts i1 auf verlag-v1.proxy.aai.mpg.de zu, so wird er z.B. an die Instanz „MPG-AAI IP Proxy Göttingen-1“ verwiesen, und erhält im Beispiel die Ausgangs-IP-Adresse 172.16.0.20. Ein Benutzer desselben Instituts der danach auf verlag-v1.proxy.aai.mpg.de zugreift, wird beispielsweise an „MPG-AAI IP Proxy Göttingen-2“ geleitet, und erhält die Ausgangs-IP-Adresse 172.16.0.21. Fällt die Instanz „MPG-AAI IP Proxy Göttingen-1“ aus, so kann der erste Benutzer direkt auf die Instanz „MPG-AAI IP Proxy Göttingen-2“ umgeleitet werden. Der EZproxy leitet ihn dabei, wie in Abbildung 4 gezeigt, an den IdP seines Heimatinstituts um, an dem er bereits eine Sitzung aufgebaut hat.

Daher muss sich der Benutzer nicht erneut anmelden und kann trotz des Ausfalls der ersten Instanz weiter mit den vom Verlag v1 bereitgestellten Ressourcen arbeiten. Durch den nginx Server werden so sowohl Ausfälle eines Standorts als auch Wartungsarbeiten innerhalb eines Rechenzentrums adressiert.

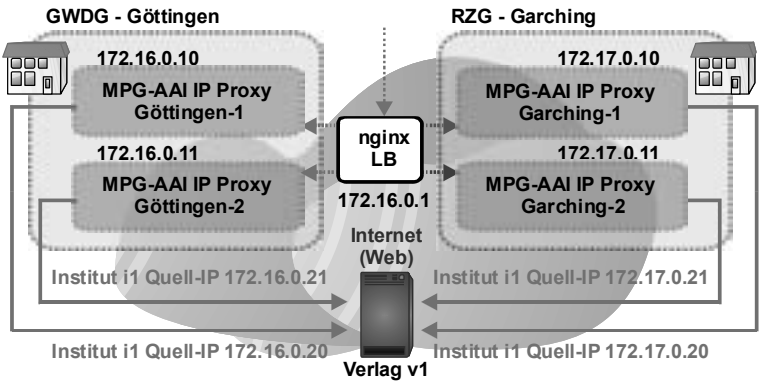


Abbildung 5: Lastverteilung und Ausfallsicherheit durch mehrere "MPG IP Proxy" Instanzen

3 Fazit und Ausblick

Die in diesem Paper vorgestellte Lösung erlaubt eine Integration von föderativen und IP-basierten Autorisierungs- und Abrechnungsverfahren innerhalb der MPG-AAI Föderation der Max-Planck-Gesellschaft. Dadurch wird eine sanfte Migration zu föderativen bzw. SAML-basierten Zugriffskontrollverfahren über alle von den Max-Planck-Instituten benötigten Verlagen ermöglicht. Für die Benutzer wird so, unabhängig von der IP-Adresse des verwendeten Web-Clients, ein Zugriff auf die Ressourcen der Verlage realisiert. Die Benutzer erhalten auf diese Weise ein Single Sign-On über IP- und bereits föderativ autorisierende Verlage. Für die Verlage und die Max-Planck Digital-Library als Bibliotheksdienstleister der Max-Planck-Gesellschaft wird darüber hinaus weiterhin eine differenzierte Abrechnung und Autorisierung der einzelnen Institute gewährleistet. Durch die im Abschnitt 2.2 vorgestellten verteilten Instanzen an den Standorten Garching und Göttingen, werden sowohl Performanz-Engpässe als auch Ausfälle minimiert, und so das Risiko des Proxy als zentrale Fehlerquelle reduziert. Ein Nachteil der Lösung besteht allerdings in dem Verbrauch von IP-Adressen für die teilnehmenden Institute. Neben diesem Nachteil erfordert auch die derzeit fehlende Anpassung der vom Proxy ausgelieferten Inhalte (z.B. werden Links in RSS Feeds nicht automatisch auf das Format http://<verlag>.ezproxy.aai.mpg.de umgesetzt), sowie die Terminierung von HTTPS Sitzungen am Proxy nach wie vor langfristig eine vollständige Migration hin zu vollständig föderativen Autorisierungs- und Abrechnungsverfahren. Aus diesem Grund arbeitet die Max-Planck-Gesellschaft zusammen mit anderen Forschungseinrichtungen derzeit an einer Erweiterung der bestehenden Standards für föderative Authentifizierung und Autorisierung (basierend auf SAML und insbesondere Shibboleth) um Accounting Attribute. Ein Vorschlag für ein geeignetes Accounting-Attribut eduPersonUsageSubset wurde bereits erstellt [EPUS].

Dieser soll nun gemeinsam mit den Entwicklern von Shibboleth sowie mit der Directory Working Group des Internet2 Middleware Architecture Committee for Education (MACE-Dir) im Hinblick auf eine mögliche Integration in die eduPerson Spezifikation diskutiert werden. Neben diesem Vorschlag existiert z.B. mit dem dfnEduPersonCostCenter [DEP] Attribut der dfnEduPerson des DFN-Vereins ein weiterer Lösungsansatz für die differenzierte Abrechnung unterschiedlicher Einrichtungen innerhalb einer Shibboleth-Föderation. Welche Erweiterung zukünftig für das Accounting in Shibboleth-basierten Föderationen verwendet werden sollte, hängt vorrangig von der Akzeptanz durch die Verlage ab. Unabhängig von der konkreten Realisierung des Accountings ist jedoch vom momentanen Standpunkt nicht absehbar ab wann alle Verlage ihre IP-basierte Zugriffskontrolle abgelöst haben. Gemeinsam mit dem bereits existierenden IdP Proxy [Rieg09] der Max-Planck-Gesellschaft ermöglicht der MPG-AAI IP Proxy bis dahin sowohl die Integration von Instituten als auch von Verlagen, die bislang noch nicht in der Lage sind Shibboleth bzw. SAML zu unterstützen.

Literaturverzeichnis

[Eggl08] Eggleston, H.: Introduction to Electronic Resources and Remote Access Issues, http://www.escholarship.org/uc/item/0hc172sp, abgerufen am 14.1.2010.

[DEP] DFN-AAI Technische und organisatorische Voraussetzungen – Attribute für den Bereich E-Learning,https://www.aai.dfn.de/fileadmin/documents/attributes/200811/DFN-AAI_E-Learning-Attribute_V.1.0.pdf, abgerufen am: 14.1.2010.

[DV] DFN-AAI Einfacher Zugang zu geschützten Ressourcen – Service-Provider, https:// www.aai.dfn.de/verzeichnis/service-provider/, abgerufen am 14.1.2010.

[EPUS] Egger, M.; Palzenberger, M.; Rieger, S.; Schier, H.: eduPersonIUsageSubset https://idp.rzg.mpg.de/mediawiki/images/2/21/Discrimination-Attribute.doc, abgerufen am 24.3.2010.

[EZp] OCLC EZproxy authentication and access software, http:// www.oclc.org/ezproxy/, abgerufen am 14.1.2010.

[Mike04] Mikesell, B. L.: Anything, Anytime, Anywhere: Proxy Servers, Shibboleth, and the Dream of the Digital Library. In: (Mahoney, P. B., Hrsg.): Proceedings of The Eleventh Off-Campus Library Services Conference, The Haworth Information Press 2004; S. 315-326.

[Morg04] Morgan, R. L.; Cantor, S.; Hoehn, W.; Klingenstein, K.: Federated Security: The Shibboleth Approach, EDUCAUSE Quarterly, Vol. 27, 2004, S. 12-17.

[MPAAI] MPG: MPG-AAI, https://aai.mpg.de, abgerufen am: 14.1.2010.

[nginx] HTTP reverse proxy server, http://nginx.org/en/, abgerufen am 14.1.2010.

[RiNe07] Rieger, S.; Neumair, B.: Towards usable and reasonable Identity Management in heterogeneous IT infrastructures. In: Proceedings of the 10th IFIP/IEEE International Conference on Integrated Network Management, 2007, S. 560-574.

[Rieg09] Rieger, S.: Benutzerzentrierte Lokalisierung für den Einsatz in Shibboleth-basierten Föderationen. In (Müller, P.; Neumair, B.; Dreo Rodosek, G., Hrsg.): Proc. 2. DFN-Forum Kommunikationstechnologien, München 2009. Gesellschaft für Informatik , Bonn, 2009; S. 13-22.

[SAML] OASIS: Security Services (SAML) TC, http://www.oasis-open.org/committees/tc_home .php?wg_abbrev=security, abgerufen am: 14.1.2010.

[Squid] Squid Optimising Web Delivery, http://www.squid-cache.org/, abgerufen am 14.1.2010.

[vasc] Verteilte Authentifizierung, Autorisierung und Rechteverwaltung (AAR), http://aar. vascoda.de, abgerufen am: 14.1.2010.

Integrierter Shibboleth Identity Provider auf Basis verteilter Identitätsdaten

Sebastian Labitzke, Michael Simon, Jochen Dinger

{sebastian.labitzke, michael.simon, jochen.dinger}@kit.edu

Abstract: Typischerweise erlauben Shibboleth-basierte Authentifikations- und Autorisationsinfrastrukturen (AAI), wie die DFN-AAI, nur *einen* Identity Provider (IdP) für *eine* teilnehmende Organisation, um den Wartungsaufwand seitens des AAI-Betreibers möglichst gering zu halten. Ferner wahrt dies die Benutzerfreundlichkeit, da so das IdP-Verzeichnis minimal ausfällt, aus dem Nutzer vor der Authentifikation die passende Organisation auswählen müssen. Allerdings liegen in großen Einrichtungen Identitätsdaten häufig in verteilten Datenquellen vor und sind nicht über eine zentralisierte Schnittstelle verfügbar. Die Shibboleth IdP-Implementierung ist jedoch in der Anbindung verteilter Datenquellen limitiert. In dieser Arbeit werden mögliche Konzepte zur Integration eines IdP in eine Organisation mit verteilten Identitätsdaten vorgestellt und bewertet. Dabei werden für die Authentifikation bestehende Ansätze untersucht. Bislang nicht erfüllten Anforderungen konnte durch zwei Entwicklungen, einem *Shibboleth Login Handler* und einem *JaaS Dispatcher Module*, nachgekommen werden. Darüber hinaus wird gezeigt, wie sich die Shibboleth-Attributlieferung in ein bestehendes Identitätsmanagementsystem integrieren lässt. Die Umsetzbarkeit der vorgestellten Integrationslösungen wird abschließend am Beispiel des Karlsruher Instituts für Technologie verdeutlicht.

1 Einleitung

Als dezentrales Authentifikations- und Autorisationssystem für Browser-basierte Web-Dienste hat sich im Bereich der Forschung und Lehre die Spezifikation Shibboleth und das zugehörige Softwareprodukt der „Internet2 Middleware Initiative“[1] etabliert. Nutzer werden dabei durch Shibboleth Identity Provider (IdP) authentifiziert. Ferner liefern IdPs Attribute als Basis für eine Autorisationsentscheidung an Web-Dienste. Somit kann die Implementierung des Web-Dienstes auf dessen Kernfunktionalitäten beschränkt bleiben und ein dienstübergreifendes Single-Sign On wird ermöglicht. Weiterführende Informationen zum Ablauf von Shibboleth-Authentifikationen und -Autorisationen finden sich unter anderem auf den Web-Seiten der Switch AAI[2].

Zur Kollaboration über Organisationsgrenzen hinweg werden zudem Authentifikations- und Autorisationsinfrastrukturen (AAIs) aufgebaut. Diese übernehmen die Verwaltung der Shibboleth Meta-Daten, die für den Einsatz von Shibboleth notwendig sind und ansonsten bidirektional zwischen Betreibern von Web-Diensten und IdP-Betreibern ausgetauscht

[1] http://shibboleth.internet2.edu/
[2] http://switch.ch/aai/demo/

werden müssten. Die Betreiber solcher AAIs, wie das Deutsche Forschungsnetz (DFN), stellen einen sogenannten Discovery Service zur Verfügung, über den einem Nutzer eine Auswahl an teilnehmenden Organisationen und damit deren IdPs zur Verfügung gestellt wird. So kann ein Nutzer die Einrichtung wählen, bei der für ihn ein entsprechendes Nutzerkonto eingerichtet wurde, und wird zur Authentifikation zu dessen IdP weitergeleitet.

Da die Auswahl des IdPs möglichst übersichtlich gehalten werden soll, streben AAIs an, nur jeweils einen IdP als Authentifikationsdienst einer Organisation zu verzeichnen. Diese Restriktion kann Organisationen, die an der AAI teilnehmen wollen, vor Herausforderungen stellen. Shibboleth IdPs sind in den Möglichkeiten zur Anbindung verteilter Identitätsdaten eingeschränkt und die Forderung nach einem IdP, der alle relevanten Nutzergruppen einer Organisation authentifizieren und Attribute für diese zur Verfügung stellen kann, ist insbesondere dann problematisch, wenn keine organisationsweite Nutzerkontenverwaltung existiert oder ein Identitätsmanagement (IdM) einen einheitlichen Zugriff gewährleistet. Zur Authentifikation von Nutzern aus verschiedenen Nutzerverwaltungen sieht Shibboleth das AAI-Konzept vor. Würde demnach organisationsintern auf mehreren Nutzerverwaltungen eine AAI aufgebaut, müssten alle darin etablierten IdPs im Discovery Service einer übergeordneten AAI verzeichnet werden, um auch an dieser teilzunehmen. Dies würde jedoch der Forderung nach einem IdP pro teilnehmender Organisation widersprechen. Abbildung 1 visualisiert das dargestellte Problem noch einmal.

Wie in Abschnitt 2 näher erläutert wird, gibt es bereits Möglichkeiten, einen IdP mit verteilten Datenquellen zu konfigurieren. Diese Möglichkeiten sind jedoch entweder in ihrer Flexibilität eingeschränkt, gehen mit Einbußen bezüglich der Leistung einher oder bedingen zusätzliche Nutzerinteraktionen bei der Authentifikation. Die Entwicklung individueller Module und die IdP-Integration nach den in diesem Papier vorgestellten Konzepten erfüllen entsprechende Anforderungen und bedeuten eine Reduktion des betrieblichen Aufwands. Es werden zwei flexibel einsetzbare Module zur Realisierung der Authentifikation sowie ein Konzept zur Integration eines IdP in bestehende IdM-Systeme vorgestellt. Dabei wird diskutiert unter welchen Voraussetzungen und an welcher Stelle individuelle Module zum Einsatz kommen können und entsprechende Umsetzungen präsentiert.

Der folgende Abschnitt 2 untersucht und bewertet ausgewählte bestehende Ansätze. Das erarbeitete Lösungskonzept und die implementierten Authentifikationsmodule werden im Abschnitt 3 vorgestellt. Bevor in Abschnitt 5 die Ergebnisse zusammengefasst werden und auf die zukünftigen Shibboleth-Vorhaben am Karlsruher Institut für Technologie (KIT)

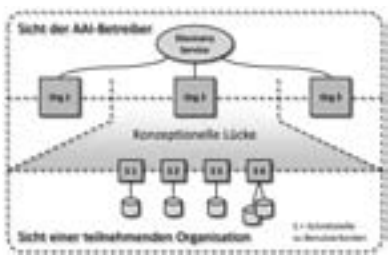


Abbildung 1: Konzeptionelle Lücke zwischen Sicht der AAI-Betreiber und Organisationen

eingegangen wird, wird in Abschnitt 4 ein Blick auf die Shibboleth-Infrastruktur am KIT geworfen und Aspekte wie das Clustering skizziert.

2 Bestehende Lösungsansätze

Die Authentifikation und Attributlieferung durch einen einzelnen Shibboleth IdP ist genau dann problematisch, wenn eine Einrichtung aus Organisationseinheiten mit eigenen Nutzerverwaltungen und damit verteilt vorliegenden Identitätsdaten besteht. Im Folgenden werden existierende Möglichkeiten vorgestellt und bewertet, durch die der Zugriff auf verteilte Identitätsdaten realisiert werden kann.

Eine Möglichkeit bietet der bei Shibboleth zum Einsatz kommende *JAVA Authentication and Authorization Service* (JaaS) [Mah03]. Schnittstellen zu multiplen Nutzerverwaltungen können damit sukzessiv durchlaufen werden, um die passende Quelle für eine Authentifikation zu finden. Hierfür wird eine Liste verschiedener Authentifikationsschnittstellen aufgebaut. Es existieren bereits JaaS-Module, um zum Beispiel gegen LDAP-Schnittstellen zu authentifizieren oder Kerberos Authentifikationen zu integrieren. Den konfigurierten Schnittstellen werden zusätzlich Attribute hinzugefügt, die beispielsweise anzeigen, ob eine erfolgreiche Authentifikation gegen eine Schnittstelle hinreichend oder notwendig ist.

Die Anbindung von Authentifikationsschnittstellen mit JaaS funktioniert jedoch nur dann ohne individuelle Implementierung, wenn bereits JaaS-Module für die zu konfigurierenden Schnittstellen verfügbar sind und keine komplexere Logik als das sequentielle Durchlaufen dieser notwendig ist. Soll mittels proprietärer Schnittstellen wie Web Services, CGIs, Skripten etc. auf eine Quelle zugegriffen oder zusätzliche Restriktoren überprüft werden, können individuelle JaaS-Module implementiert werden. Das JaaS-Modul wird analog den existierenden Modulen in der Datei *login.config* konfiguriert und das als *.jar* kompilierte Modul in das *war*-File des IdP in den Ordner *WEB-INF\lib* abgelegt.

Mit dem Einsatz mehrerer JaaS-Module, wächst jedoch die Latenz einer Authentifikation um die Länge der Antwortzeiten von Datenquellen, gegen deren Schnittstellen eine Authentifikation nicht erfolgreich verlief, bevor die Authentifikationsanfrage an die passende Quelle gereicht wurde. Eine Vorauswahl der Authentifikationsquelle, zum Beispiel anhand eines Schemas für Benutzernamen, ist nicht vorgesehen.

Alternativ wurden bereits verschiedene proprietäre Module, vor allem Servlet-Filter und Shibboleth Login Handler, entwickelt. Die Universitätsbibliothek Freiburg setzt das Modul *myLogin*[3] als Erweiterung zum Shibboleth IdP ein. *myLogin* ermöglicht die Anbindung mehrerer Nutzerkontenverwaltungen und bietet dem Nutzer im Anschluss an die Auswahl der Heimateinrichtung beim Discovery Service der AAI eine Auswahl der zur Verfügung stehenden organisationsinternen Quellen an. So kann ein Nutzer stets den Nutzerkontenpool auswählen, gegen den er sich authentifizieren möchte, respektive für den er einen Login besitzt. Dieses Modul ist von besonderem Vorteil, wenn ein Nutzer verschiedene

[3] https://mylogin.uni-freiburg.de

Nutzerkonten besitzt, mit denen jeweils unterschiedliche Attribute und Rechte verknüpft sind. Nach erfolgreichem Login werden so je nach zuvor getätigter Auswahl die zum Nutzerkonto gehörigen Attribute an die Service Provider geliefert.

Mit *myLogin* wurde eine Hierarchisierungsstufe bei der Auswahl der Authentifikationsquelle eingeführt. Nachteilig ist jedoch, dass unter Einsatz dieses Moduls den Nutzern nach dem Discovery Service eine weitere System-Interaktion aufgebürdet wird. Die Wiederverwendbarkeit von *myLogin* ist zudem dann eingeschränkt, wenn interne Organisationsstrukturen vorhanden sind, bei denen die Nutzer ihr Nutzerkonto nicht eindeutig einem angegebenen Nutzerkontenpool (z.B. Rechenzentrum, Bibliothek, Klinikum...) zuordnen können, so dass ein Ausprobieren der Quellen notwendig wäre. Insbesondere ist dies der Fall, wenn mit einem Konto zentrale Dienste genutzt werden und der zugehörige Nutzername keinen Aufschluss über die das Nutzerkonto verwaltende Organisationseinheit gibt.

Um *eine* Schnittstelle zum Zugriff auf verteilte Daten zu etablieren, kann alternativ ein virtuelles Verzeichnis oder ein Meta-Directory aufgebaut werden, in das alle notwendigen Attribute sowie Informationen zu Nutzerkonten und Passwörter repliziert werden. Ein derartiges Verzeichnis würde als einzige Quelle im IdP konfiguriert werden. Für Einrichtungen, die bereits eines dieser beiden Verzeichnisarten betreiben, kann die Anbindung dieses eine Alternative zu oben genannten Lösungen sein. Gegen die Etablierung eines solchen Verzeichnisses speziell für die Shibboleth-Infrastruktur spricht jedoch der zu erwartende erhebliche Aufwand für Betrieb und Wartung. Insbesondere ohne ein umfassendes IdM-System kann der Datenbestand eines Meta-Directory nur mit zusätzlichem Aufwand auf einem aktuellen Stand gehalten werden.

3 Authentifikationsmodule und Attributprovisionierung

Um den Aspekten Flexibilität, Geschwindigkeit und Nutzerkomfort bei der Anbindung verteilter Identitätsdaten gerecht zu werden, kann die Notwendigkeit zu einer individuellen Lösung bestehen. Die erarbeiteten Lösungsvorschläge für die Authentifikation sowie die integrative Bereitstellung von Attributen für den Shibboleth IdP werden im Folgenden getrennt voneinander vorgestellt.

3.1 Authentifikationsmodule

Für die konzipierten Authentifikationsmodule werden folgende Annahmen bzw. Anforderungen zu Grunde gelegt. Organisationseinheiten, die ihre Accounts eigenständig verwalten, sollen dazu auch nach der Etablierung eines IdP in der Lage sein, ohne zusätzliche Prozesse etablieren zu müssen, um die Shibboleth-Infrastruktur mit aktuellen Daten zu versorgen. Ferner ist die Replikation eines Passworts in eine zweite Datenquelle, neben dem Sicherheitsfaktor und dem erhöhten Aufwand für Passwortänderungsprozesse, technisch oft nicht möglich. Außerdem ist zu beachten, dass im Bibliotheksbereich häufig mit einer IP-Überprüfung als hinreichende Authentifikation der Nutzer gearbeitet wird

[ORBL09]. Mit dem Einsatz von Shibboleth kann die IP-basierte gegen eine personalisierte Authentifikation ersetzt werden, jedoch dürfen z.B. sogenannte Library-Walk-In-Nutzer nur von Rechnern der Bibliothek auf lizensierte Inhalte zugreifen, so dass eine aus beiden Verfahren kombinierte Authentifikation ermöglicht werden sollte.

Ferner war das Ziel der Entwicklung von Authentifikationsmodulen die passende Nutzerverwaltung zu identifizieren, bevor die Authentifikationsanfrage an eine der konfigurierten Schnittstellen gerichtet wird. Da die Datenquellen so nicht sequentiell abgearbeitet werden müssen, vermindert dies die Verzögerungszeit der Authentifikation. Voraussetzung für die automatisierte Auswahl der Datenquelle ist, dass die unterschiedlichen Identifikatoren wie E-Mail-Adressen und Nutzerkennungen eindeutig den Datenquellen zuordenbar sind. Für die Entwicklung der im folgenden vorgestellten Module sollte die Identitfikation über reguläre Ausdrücke in einer Konfigurationsdatei eingestellt werden können.

Insofern ergeben sich folgende spezifischen Anforderungen:

- Wahrung der Autonomie von Organisationseinheiten bezüglich ihrer Nutzerkonten
- Zugriff auf verteilte Identitätsdaten mit minimaler Latenz beim Nutzerlogin
- Keine Replikation von Passwörtern in Shibboleth-spezifische Datenbanken
- *Ein* IdP, der alle abzudeckenden Nutzergruppen authentifizieren kann
- Automatisierte, konfigurierbare Identifikation der zum Nutzer gehörigen Quelle
- Einbezug der Nutzer-IP-Adresse in die Authentifikationsentscheidung (optional)

Abbildung 2 zeigt zum einen die Anbindung verteilter Identitätsdaten mit bestehenden Lösungen, wie sie in Abschnitt 2 vorgestellt wurden. Zum anderen werden die im Rahmen dieser Arbeit erweiterten Konzepte sowie entstandene Komponenten visualisiert, die durch einen Stern gekennzeichnet sind. Dargestellt ist im ersten Teil eine Anbindung verteilter Datenquellen mit JaaS und einer sequentiellen Abarbeitung der Authentifikationsquellen, wie es ein IdP vorsieht. Im zweiten Teil der Abbildung ist visualisiert, wie ein Zugriff auf verteilte Daten durch den Einsatz eines virtuellen Verzeichnisses ermöglicht wird.

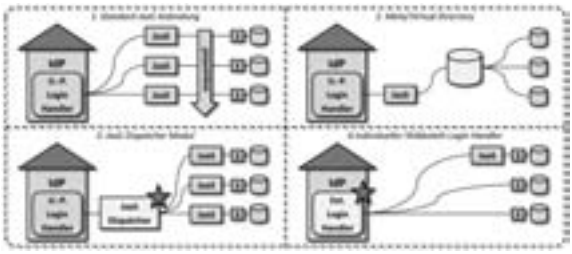


Abbildung 2: Konzepte zur Anbindung verteilter Identitätsdaten

JaaS Dispatcher Module: Um die zu erwartende Verminderung der Authentifikationsgeschwindigkeit durch ein sequentielles Abarbeiten mehrerer in der Datei *login.config* konfigurierter JaaS-Module zu umgehen, wurde ein *JaaS Dispatcher Module* entwickelt, wie es im dritten Teil der Abbildung 2 visualisiert ist. Dieses wendet reguläre Ausdrücke, die in der Datei *login.config* konfiguriert werden können, auf die Nutzernamen an und entscheidet, an welches weitere JaaS-Modul die Authentifikation delegiert werden muss.

Das Dispatcher-Modul ist ebenfalls ein JaaS-Modul und implementiert das Interface *LoginModule*. Für die nachgelagerten JaaS-Module wird jeweils ein eigener Namensraum in der Datei *login.config* konfiguriert und diese in der Methode *initialize* des Dispatcher-Moduls, zusammen mit den regulären Ausdrücken, eingelesen. In der Methode *login* wird anschließend ein entsprechender *LoginContext* aufgebaut und die Authentifikation an diesen delegiert. Der Aufruf des zum *LoginContext* gehörigen Moduls verläuft analog dem Aufruf des ersten JaaS-Moduls durch den Shibboleth IdP selbst.

Extended Login Handler: Die Shibboleth IdP-Implementierung stellt den JaaS-Modulen lediglich den Nutzernamen und das Passwort mittels sogenannter *Callback Handler* zur Verfügung, jedoch keine weiteren Attribute aus der Anfrage des Nutzers. Um zusätzlich die IP-Adresse des Nutzers in den Authentifikationsprozess einbeziehen zu können, kann der *Extended Login Handler* eingesetzt werden. Dieser individuell implementierte Shibboleth Login Handler ist im vierten Teil der Abbildung 2 visualisiert. Er ist durch die Replikation und entsprechende Anpassungen der Klassen[4] des *Username Password-Login Handler* in separate Namensräume, einer Erweiterung der Klasse *BaseSpringNamespaceHandler* und dem Ausbau der Methode *authenticateUser* der Klasse *UsernamePasswordLoginServlet* realisiert worden. In diese Methode wurde, analog dem Ansatz mit einem JaaS-Dispatcher-Modul, die Auswahl der Datenquelle und die Logik für die Authentifikation eingebracht. Auf die IP-Adresse des Nutzers wird über den Http-Request durch den Aufruf *request.getRemoteAddr* zugegriffen und der entsprechende Wert optional in die Authentifikationslogik integriert. Die Authentifikation gegen die unterschiedlichen Schnittstellen der Identitätsdaten kann über das konfigurierte JaaS-Modul oder über direkte Zugriffe auf proprietäre Schnittstellen implementiert werden.

Alternativ ist es möglich weiterhin das *JaaS Dispatcher Module* zu nutzen und lediglich die Übergabe der IP-Adresse des Nutzers in den Shibboleth Login Handler zu integrieren. Die Bereitstellung der IP-Adresse kann als zusätzlicher Callback implementiert werden, indem die Methode *handle* der Klasse *UsernamePasswordLoginServlet* entsprechend erweitert wird. In jedem Fall ist für den Einbezug der IP-Adresse des Nutzers die Ergänzung eines individuellen Login Handler notwendig.

Rückblickend auf die gestellten Anforderungen wahren beide vorgestellten Lösungen die Autonomie der Organisationseinheiten bezüglich ihrer Nutzerkonten, da direkt gegen diese authentifiziert wird und aus einer Kontensperrung eine umgehende Sperrung des Shibboleth-Zugangs folgt. Der Zugriff auf bestehende Nutzerverwaltungen erspart des Weiteren die Replikation von Passwörtern in eine dedizierte Shibboleth-Authentifikationsquelle.

[4] UsernamePasswordLoginHandler, UsernamePasswordLoginServlet, UsernamePasswordLoginHandlerBeanDefinitionParser, UsernamePasswordLoginHandlerFactoryBean

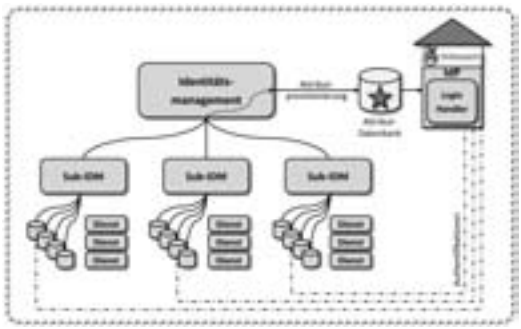


Abbildung 3: Integrierte Attributprovisionierung für einen Shibboleth IdP

Durch den Einsatz der vorgestellten Lösungen, können mit *einem* IdP verteilt vorliegende Nutzerkonten zur Authentifikation genutzt werden. Da beide Module automatisiert und anhand konfigurierbarer regulärer Ausdrücke eine Vorauswahl der Authentifikationsquelle treffen, werden lediglich Anfragen an für ein Nutzerkonto zuständige Quellen gestellt und andere Quellen übersprungen, wodurch eine Leistungsoptimierung erreicht werden konnte. Durch die Möglichkeit des Zugriffs auf die IP-Adresse im *Extended Login Handler* konnte abschließend auch der optionalen Anforderung an den Einbezug dieses Merkmals in die Authentifikationsentscheidung gerecht werden. Ist ein solcher Einbezug nicht notwendig, ist der Einsatz des *JaaS Dispatcher Module* vorzuziehen, da dieser keinen Eingriff in den Shibboleth-Code erfordert und zur Integration lediglich konfiguriert werden muss.

3.2 Integrierte Attributprovisionierung

Für das Konzept zum Zugriff auf Nutzerattribute wird im Folgenden angenommen, dass eine Organisation in Einheiten aufgespalten und ein IdM-System im Einsatz ist [SHH08]. Dieses System versorgt die Organisationseinheiten mit personenbezogenen Daten der Verwaltungseinheiten und kann Daten eines Sub-Systems in andere replizieren. Die Verwaltung lokaler Nutzerkonten sowie die Anbindung von Diensten obliegen jedoch den einzelnen Einheiten. Abbildung 3 zeigt einen solchen IdM-Aufbau mit einem bereits integrierten Shibboleth IdP (rechts im Bild). Der IdP wurde mit einem individuell implementierten Authentifikationsmodul versehen, das nach den Konzepten aus Abschnitt 3.1 implementiert wurde und die Schnittstellen zu Nutzerverwaltungen der einzelnen Organisationseinheiten anbindet. Attribute, die an Web-Dienste ausgeliefert werden sollen, werden dagegen in einer dedizierten Attribut-Datenbank dem IdP aufbereitet und im erforderlichen Schema zur Verfügung gestellt. Im Unterschied zu einem Meta-Directory werden hier nur die für die Shibboleth-Attributlieferung benötigten Daten abgelegt, andere Daten und Passwörter werden nicht repliziert.

Es bietet sich an benötigte Attribute zu allen Nutzerkonten in einer solchen dedizierten Datenbasis zu aggregieren, da einerseits eine Shibboleth-seitige Konfiguration des Mappings von Attributen in das gewünschte Zielschema der AAI (beispielsweise *eduPerson*)

entfällt. Die Übersichtlichkeit der Shibboleth-Konfiguration bleibt gewahrt und der initiale Konfigurationsaufwand dafür wird minimiert. Ferner liegen einige benötigte Attribute, insbesondere für das *eduPerson*-Schema, nicht in den verteilten Nutzerverwaltungen vor und können demnach nicht ad-hoc eingeholt werden, sondern sind in Abhängigkeit der Nutzergruppe lediglich implizit bekannt. Hierzu zählen zum Beispiel Attribute, die Beziehungen der Nutzer zur Organisation oder Rechte innerhalb der AAI repräsentieren.

3.3 Bewertung

Zunächst widersprüchlich könnten die auseinanderlaufenden Konzepte für die Authentifikation und die Attributlieferung scheinen. Bei der Authentifikation ist das verfolgte Ziele auf verteilt vorliegende Identitätsdaten zuzugreifen, Attribute werden hingegen aggregiert und zentral vorgehalten. Die Alternative auf Seiten der Authentifikation wäre, die Nutzerkonten und damit auch sensible Informationen wie Passwörter zentral und redundant vorzuhalten. Dagegen spricht jedoch nicht nur das Risiko des Transports der Passwörter von einer in eine andere Datenbank, sondern auch die verminderte Entscheidungsfreiheit der Organisationseinheiten über die Kontoberechtigungen. Würden die Nutzerkonten in eine zentrale Datenbasis repliziert, müssten Mechanismen geschaffen werden, die bei einer Kontensperrung oder einem Rechteentzug auch die Möglichkeit der Shibboleth-Authentifikation für betroffene Nutzer unterbinden. Mit der verteilten Haltung der Nutzerkonten wird dies implizit vollzogen, wenn in den Organisationseinheiten ein Kontostatus verändert wird. Ein virtuelles Verzeichnis würde dem entgegen kommen. Jedoch bedeutet der Einsatz dieser zusätzlichen Komponente mehr betrieblichen Aufwand und damit höhere Betriebskosten, als ein in Shibboleth integriertes Modul aufwirft. Auf technischer Seite stellt der Einsatz eines virtuellen Verzeichnisses auch einen Aufbau einer weiteren Fehlerquelle für die Authentifikation dar, die stets überwacht werden muss. Der Integrationsaufwand für den Einsatz eines Authentifikationsmoduls fällt hingegen sehr gering aus.

Der Aufwand für den Aufbau und Betrieb einer dedizierten Attribut-Datenbank ist ebenfalls gering. Alternativ könnte auch die Attributlieferung durch einen dezentralen Ansatz realisiert werden. Wie bereits beschrieben, ist jedoch einer der Vorteile, dass mit einem aufbereiteten Satz von Daten die Geschwindigkeit einer Authentifikation erheblich gesteigert werden kann. Zum Teil aufwändige Berechnungen von Attributen zur Laufzeit würden die Bereitstellung von Attributen erheblich mindern. Ein weiterer Vorteil der dedizierten Attributquelle birgt die Verlagerung der Schemakonvertierung zum IdM-System, anstatt dies durch den Shibboleth IdP durchführen zu lassen. Attribute können so nicht nur automatisiert aktuell gehalten werden, die zum Teil komplexe Schemakonvertierung, zum Beispiel in ein AAI-weit gültiges Attributschema durch die Konfiguration des IdPs, wird durch die wesentlich flexiblere Konvertierung durch ein IDM-System ersetzt. Der Verzicht auf eine zusätzliche Erweiterung der Shibboleth-Software und damit der Einsatz einer dedizierten Datenbasis für Attribute ist abschließend auch dadurch begründet, dass es Nutzergruppen geben kann, für die Attribute nur implizit bekannt sind und nicht explizit in den Datenquellen der verschiedenen Nutzerverwaltungen vorliegen.

4 Shibboleth am KIT

Am KIT[5] ist ein föderatives IdM-System etabliert, das Organisationseinheiten mit Daten versorgt, die ihrerseits diese Daten anreichern und in den eigenen IT-Systemen einsetzen können, um Dienste anzubieten. Diesem Identitätsmanagement kommt eine besondere Bedeutung zu, da sowohl der Campus Süd (ehem. Universität) mit ca. 4.000 Mitarbeitern und ca. 20.000 Studierenden sowie der Campus Nord (ehem. Forschungszentrum) mit ca. 4.000 Mitarbeitern jeweils eine eigenständige Personalverwaltung betreiben. Durch die Gründung des Steinbuch Centre for Computing (SCC) als gemeinsames Rechenzentrum und dem Aufbau eines föderativen IdM-Systems sind viele Herausforderungen bezüglich der bestehenden und neu hinzukommenden Nutzerkonten überwunden worden. Dennoch liegt hier eine bereits gegebene Aufteilung in Organisationseinheiten vor, die Vorhaben im Bereich des Identitätsmanagement erschweren und für die Etablierung von Shibboleth den Einsatz der skizzierten Lösung nötig machen.

Aus dem Verständnis der Einrichtung als eine Föderation seiner eigenen Satelliten entstand das föderative IdM-System des KIT [SHH09]. Die personenbezogenen Daten, die Organisationseinheiten zur Verwaltung von Nutzerkonten benötigen, werden vom zentralen IdM-System an die Satelliten IdM-Systeme verteilt. Dienste, die den Verantwortungsbereich einer einzelnen Organisationseinheit übersteigen, wie ein Shibboleth IdP, werden direkt vom föderativen IdM-System gespeist. Eine Integration eines Shibboleth IdPs sowie dessen Zugriff auf getrennt verwaltete Nutzerkonten der beiden Organisationsteile des KIT und darüber hinaus deren Organisationseinheiten konnten mit dem oben vorgestellten Konzept realisiert werden. Die verschiedenen Datenquellen wurden für Authentifikationen durch einen *Extended Login Handler* angebunden und eine dedizierte Attribut-Datenbank eingerichtet, die durch das IDM-System provisioniert wird.

Um den Shibboleth IdP hochverfügbar anbieten zu können, wurden zwei Hardware-basierte sowie zwei virtuelle Maschinen aufgesetzt. Die IdPs werden in einem dedizierten virtuellen LAN betrieben und ein F5 BIG-IP Loadbalancer[6] voran geschaltet. Diese Hardware stellt den Zugangspunkt zur Shibboleth-Infrastruktur. Mit Terracotta[7] wird zudem die Sitzungsverwaltung geclustert, so dass bestehende Nutzersitzungen bei Ausfall einer Maschine auf eine andere übertragen werden und der Nutzer innerhalb der Gültigkeit seiner Sitzung keinen erneuten Loginvorgang durchlaufen muss.

Der betriebliche Aufwand blieb durch den Einsatz des *Extended Login Handler* auf übliche Shibboleth-Betriebsaspekte (Konfiguration neuer Service Provider etc.) beschränkt und es wurden keine zusätzlichen Komponenten etabliert. Zusätzliche Authentifikationsquellen können durch die eingesetzten Module effizient hinzu konfiguriert werden. Initial nicht vorgesehene Attribute lassen sich durch den Einsatz des IdM-Systems flexibel und ebenfalls zeitnah in die etablierte Shibboleth-Attributdatenbank integrieren und durch minimale Konfigurationsänderungen des IdP an entsprechende Service Provider ausliefern.

[5] Zusammenschluss der ehem. Einrichtungen Universität Karlsruhe (TH) und Forschungszentrum Karlsruhe.
[6] http://www.f5.com
[7] http://www.terracotta.org

5 Zusammenfassung und Ausblick

Die Integration eines Shibboleth Identity Provider in bestehende IdM-Infrastrukturen erfordert unter Umständen spezifische Konzepte sowie individuelle Implementierungen, um der Forderung von AAI-Betreibern nach einem IdP pro teilnehmender Organisation gerecht zu werden. In dieser Arbeit wurden Konzepte vorgestellt, mit denen die Authentifikationsmechanismen und Attributlieferung eines Shibboleth IdP an durch Organisationseinheiten verteilt verwaltete Identitätsdaten angebunden werden können. Es wurden bestehende Ansätze diskutiert, die jedoch nicht allen Anforderungen gerecht werden. Anschließend wurden zwei Entwicklungen vorgestellt, welche die zu einem Nutzernamen passende Nutzerverwaltung anhand regulärer Ausdrücke identifizieren und die Authentifikationsanfrage direkt an die entsprechende Datenquelle richten. Durch das vorgstellte *JaaS Dispatcher Module* oder alternativ dem Einsatz des *Extended Login Handler* wird so vermieden, dass Authentifikationsanfragen an für einen Nutzer nicht zuständige Datenquellen gerichtet werden und damit die Latenz einer Authentifikation verringert. Ferner wurde eine Möglichkeit mittels des *Extended Login Handler* vorgestellt, um die IP-Adresse des Nutzers in die Authentifikationsentscheidung einzubeziehen. Abschließend wurde gezeigt, wie das Konzept am KIT umgesetzt wurde, um Shibboleth trotz verteilt vorliegender Identitätsdaten als Authentifikations- und Attributlieferdienst anbieten zu können.

Das vorgestellte Konzept zur Attributprovisionierung kann in Zukunft weiter verfeinert werden, indem die Attribut-Datenbank nicht vorprovisioniert, sondern erst nach der ersten erfolgreichen Authentifikation eines Nutzers mit dessen Attributen befüllt wird. Mit dieser Erweiterung hätten Nutzer die Entscheidungsfreiheit, ob ihre Attribute auch der Shibboleth-Infrastruktur zur Verfügung stehen sollen. Darüber hinaus würde die Attribut-Datenbank nicht mit Attributen von Nutzern gefüllt, die eine Shibboleth-Authentifikation nicht benötigen. Ferner wäre eine Optimierung denkbar, mit der nur die Attribute provisioniert werden, die für den gewünschten Dienst angefordert werden. Herausforderungen für dieses Konzept stellen die notwendige Verfügbarkeit aller potentiellen Quellen für Attribute und etwaige Minderungen der Latenz durch das Aggregieren und Konvertieren von Daten zwischen einer Authentifikation und der Auslieferung von Attribute.

Literatur

[Mah03] Qusay H. Mahmoud. Java Authentication and Authorization Service (JAAS) in Java 2, Standard Edition (J2SE) 1.4. URL: http://java.sun.com/developer/technicalArticles/Security/jaasv2/, September 2003.

[ORBL09] B. Oberknapp, A. Ruppert, F. Borel und J. Lienhard. From a pile of IP addresses to a clear authentication and authorization with Shibboleth. *Serials*, 1:28–32, 2009.

[SHH08] F. Schell, T. Höllrigl und H. Hartenstein. Federated and Service-Oriented Identity Management at a University. In *Proceedings of the 14th European University Information Systems (EUNIS 2008)*, Juni 2008.

[SHH09] F. Schell, T. Höllrigl und H. Hartenstein. Federated Identity Management as a Basis for Integrated Information Management. *it - Information Technology*, 1:14–23, 2009.

Erfahrungen und Perspektiven eines rollenbasierten IdM

Christopher Ritter, Thomas Hildmann, Odej Kao

tubIT – IT-Service-Center
Technische Universität Berlin
Einsteinufer 17
10587 Berlin
christopher.ritter@tu-berlin.de
thomas.hildmann@tu-berlin.de
odej.kao@tu-berlin.de

Abstract: Das personalisierte Dienstportal der TU Berlin basiert auf dem Identity Management (IdM) System TUBIS und verfolgt den Ansatz einer rollenbasierten Zugangsregelung. Jedes Mitglied der TU Berlin wird automatisch erfasst und mit Standardrollen ausgestattet, die im Arbeitsalltag durch Delegation, Stellvertretung oder Übertragung von Funktionen um weitere Rollen ergänzt werden können. Die wichtigste strategische Entscheidung bei der Entwicklung von TUBIS bestand darin, dass die Rollenzuordnung und -verwaltung vollständig dezentral erfolgt. Das System wird von mehr als 37000 Mitgliedern der TU Berlin täglich genutzt. Nach drei Jahren Erfahrung im Produktionsbetrieb und unzähligen Supportanfragen wird in diesem Beitrag evaluiert, ob und ggf. wie weit sich die dezentrale Rollenvergabe bewährt hat. Wurden die Vorteile erkannt und in der Breite genutzt? Oder überwiegten doch eher die Nachteile, da z.B. auch weniger IT-affine Personen mit dem System umgehen sollten aber nicht konnten, womit eine Frustrationsquelle bei den Nutzern entstanden ist? In diesem Erfahrungsbericht werden die Vor- und Nachteile einer dezentralen, gegenüber einer zentralen Rollenvergabe analysiert sowie aus Sicht der Betreiber evaluiert.

1 Einleitung

Die Veränderungen der letzen Jahre in der IT-Hochschullandschaft spiegeln den Trend zur Integration vielfältiger Universitätsbereiche wieder, die vorher weitgehend unabhängig voneinander gearbeitet haben. Der Bedarf für eine solche Integration entsteht durch die Erwartungen von Studierenden und Mitarbeitern zahlreiche Dienste durch Selbstbedienungsfunktionen zu nutzen und somit mehr Zeit für Studium und Forschung zu gewinnen. Die Umsetzung eines integrierten Dienstangebots stellt die Hochschulen wiederum vor signifikante technische und organisatorische Herausforderungen. Geschäftsprozesse und Verantwortlichkeiten sind selten umfassend dokumentiert, wodurch eine übergreifende Planung, Steuerung und Operationalisierung erschwert wird.

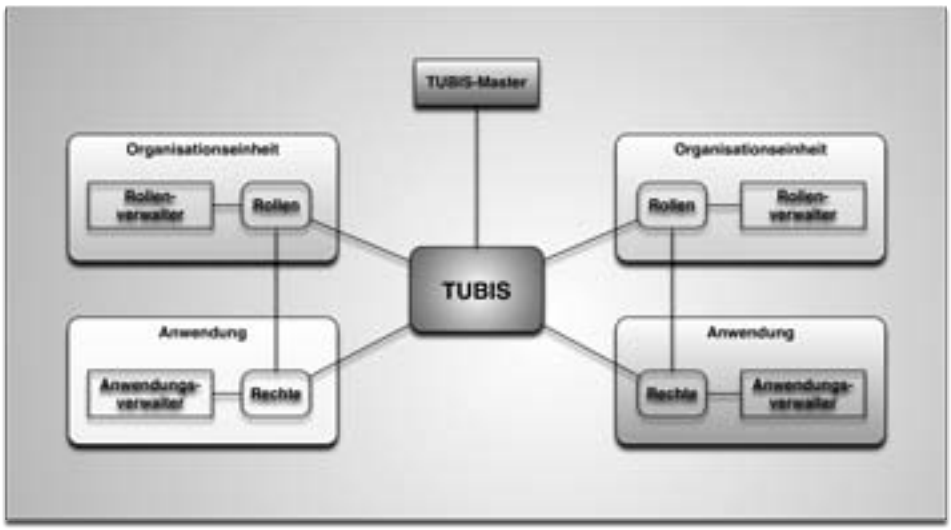


Abbildung 1: Dezentral verwaltetes, rollenbasiertes IdM „TUBIS“

Neben den notwendigen Veränderungen in der Leitungs- und Organisationsstruktur wartet noch eine Reihe von technischen Problemen auf eine Lösung. Das dominierende Thema ist in diesem Bereich ein funktionierendes System für das Identitätsmanagement. Jedes Mitglied der Universität muss eindeutig und mit allen Befugnissen, Kontexten wie etwa Status (Studierender, Mitarbeiter), Rolle (Dekan, FG-Leiter, Abteilungsleiter, …) oder Studiengang, bekannt sein, damit ein möglichst einfacher, einheitlicher Zugang zu allen für ihn relevanten Diensten möglich wird; und dies gleichgültig, ob sich die Person am Arbeitsplatz, zu Hause oder auf einer Dienstreise befindet.

An der TU Berlin wurde für die Aufgabe „Identitätsmanagement“ das universitätsweite, rollenbasierte Autorisierungssystem TUBIS entwickelt und stetig erweitert [HKR08b, HR07]. In TUBIS werden notwendige Personal- und Verwaltungsinformationen aus verschiedenen Datenquellen zusammengeführt und in ein rollenbasiertes Zugriffsmodell überführt [SBCGY99]. Alle Mitarbeiter und Studierende werden bei der Einstellung bzw. Immatrikulation erfasst. Mitarbeiter werden entsprechend der Kostenstellen den Fachgebieten automatisch zugeordnet und mit den zugehörigen Rollen ausgestattet. Der Rollenansatz ist hierbei eine geeignete Metapher, die auf den unterschiedlichen Ebenen der Universität verstanden wird. Die Herausforderung besteht darin, jedem Benutzerkreis eine eigene Sicht auf das Modell zu ermöglichen. Die grundlegende Entscheidung in der TUBIS-Philosophie ist die dezentrale Vergabe und Pflege der Rollen und Rechte. Die Grundidee dahinter ist die Abbildung des Alltagslebens und somit eine hohe Akzeptanz des Systems. Ein Leiter hat alle Rechte und delegiert diese an seine Mitarbeiter bzw. entzieht sie wieder ohne eine Interaktion mit einer anderen Organisationseinheit. Synchrone Interaktionen mit Dienstleistern sollen vermieden werden, weil sie oft zu Verzögerungen, („gefühltem“) Rechtfertigungszwang und damit zu Frustrationen führen. Den Antragstellern kann es nicht schnell genug gehen, die Dienstleister fragen sich, warum diese dringende Aufgabe so plötzlich auftaucht.

Die Benutzer können jederzeit und von überall Rechte vergeben und ihren Mitarbeitern und Gästen Zugänge zu Anwendungen oder zu einer bestimmten Infrastruktur verschaffen. Das Kooperationsmodell implementiert einen dezentralen Zugang zu zentral administrierten Systemen. Nach drei Jahren Produktionserfahrung und unzähligen Supportanfragen erfolgt eine Evaluation, ob sich die strategische Entscheidung für die dezentrale Rollenvergabe bewährt hat. Wurden die Vorteile erkannt und in der Breite genutzt oder überwiegen doch eher die Nachteile, dass z.B. auch weniger IT-affine Personen mit dem System umgehen sollten aber nicht konnten, womit eine neue Frustrationsquelle entstanden ist? Die folgenden Abschnitte geben eine Zusammenfassung der Vor- und Nachteile, die in der spezifischen Umgebung der TU Berlin wahrgenommen wurden.

Kapitel 2 wird zunächst die Vorteile eines zentral verwalteten Systems aufzeigen. Anschließend werden in Kapitel 3 die Vorteile eines dezentral verwalteten Systems beschrieben. Kapitel 4 stellt die Schlussfolgerungen aus den gesammelten Erfahrungen dar.

2 Vorteile eines zentral verwalteten Systems

Ein rollenbasiertes Zugriffssystem (RBAC) [FKC07] ermöglicht eine hochflexible und in Hinblick auf die Sicherheitspolitik neutrale Modellierung der Zugriffskontrolle. Die Flexibilität und Neutralität erkauft man durch Erhöhung der Komplexität der Zugriffskontrollkonfiguration. Auf der anderen Seite wird durch die indirekte Zuweisung von Rechten zu Benutzern über Rollen der Konfigurationsaufwand stark reduziert. Die Komplexität und Sensibilität der Konfiguration sprechen eindeutig für eine Administration durch Spezialisten. In folge des verminderten Konfigurationsaufwandes werden selbst bei großer Benutzerzahl nur wenige Spezialisten zur Administration benötigt.

Die Erfahrungen an der TU Berlin zeigen, dass viele Einrichtungen der Universität die Zugriffsverwaltung selbstverständlich als Service des IT-Dienstleistungszentrums sehen. Der IT-Dienstleister ist mit den Rechten und Rollen vertraut und besitzt den Überblick über die Auswirkungen seiner Rollenkonfiguration. Der dezentrale Rollenverwalter muss sich jeweils in eine neue Rollensemantik einarbeiten, wenn neue Anwendungen hinzukommen. Aus diesem Grund bietet es sich an, einem zentralen Rollenverwaltungsteam Anforderungen in Freitextform mitzuteilen, die diese dann in eine geeignete Rollenkonfiguration überführen. Das Zusammenführen aller Anforderungen hat ferner den Vorteil, dass Synergien vom zentralen Team erkannt und genutzt werden können.

Als Argumentation für Selbstbedienungsfunktionen und dezentrale Administration wird gern die Transparenz für die Betroffenen herangezogen. Jedoch setzt die Transparenz hier das Verständnis der Konfiguration für die Betroffenen voraus. Was bedeutet die Mitgliedschaft in der einen oder anderen Rolle? Da an dieser Stelle ohnehin Beratung durch die IT-Dienstleister nötig ist, ist der Nutzen für die Anwender begrenzt.

Die Verfügbarkeit der Administratoren kann über einen zentralen Dienst leichter organisiert werden, als in kleinen Einheiten. So ist es bei einem Team aus vier oder fünf zentralen Rollenadministratoren leicht möglich, eine Vertretungsregelung zu schaffen, die auch bei hohem Urlaubs- und Krankheitsstand den Betrieb garantieren kann, wohingegen bei der dezentralen Organisation oft nicht einmal ein Vertreter für die Rollenverwaltung definiert ist. Insofern kann die zentrale Verwaltung leicht einen Flaschenhals zu Stoßzeiten darstellen. Jedoch kann mindestens sichergestellt werden, dass immer ein Administrator verfügbar ist. Die zentrale Administration stellt ferner sicher, dass Anträge nicht nur durch das Modell, sondern händisch geprüft werden können. So können Sonderfälle durch die zentralen Mitarbeiter manuell behandelt oder Fehler in der Konfiguration schnell entdeckt und beseitigt werden. Insbesondere können durch händische Prüfung organisatorisch oder verwaltungsrechtlich unzulässige Rollenzuweisungen erkannt werden.

Hier stößt die Selbstbestimmung an ihre Grenzen. Zwar ermöglicht die dezentrale Administration in eigener Verantwortung flexibel auf äußere Begebenheiten zu reagieren, die Möglichkeiten können aber ohne eine Prüfung durch Dritte nur durch Nebenbedingungen im Modell begrenzt werden. Hierbei stellt sich die Frage, ob beispielsweise einem Hochschullehrer zugemutet werden kann, sich über alle technischen, organisatorischen und rechtlichen Konsequenzen seines Handelns im Klaren zu sein, wenn er entsprechende Rollenzuweisungen vornimmt. Hierbei darf auch nicht vergessen werden, dass die "Flexibilität" der Rollenzuweisung wiederum vom Wissen bzw. der Erfahrung im Umgang mit dem Rollensystem abhängt. Mit anderen Worten: Man kann nur konfigurieren, wozu man vom Know-how her befähigt ist. Da diese Fragen immer wieder dazu führen werden, dass der dezentrale Rollenverwalter Beratungen und Hilfestellungen von Dritten benötigt, ist das Argument der flexiblen und selbstbestimmten Administration stark relativiert.

Eine zeitnahe Implementierung von Änderungen im Rollenmodell einer Einheit ist sicherlich durch die Verfügbarkeit und Anzahl der zentralen Rollenadministratoren beschränkt. Sie kann jedoch mit organisatorischen Hilfsmitteln erreicht werden. So können Formulare erstellt werden, die die meisten Rückfragen für Aufträge reduzieren und im Idealfall komplett obsolet machen können. Diese Formulare können dann via E-Mail verschickt oder über Web-Oberflächen angeboten werden. Im Laufe der Zeit können die Antragsteller immer genauere Angaben machen, bis keine Rückfragen mehr nötig sind. Das Erlernen der neuen Techniken wird hier im Dialog mit den Mitarbeitern des IT-Dienstleisters erreicht.

Die Verteilung von Verantwortlichkeiten ist ein zentrales RBAC-Werkzeug. Der zentrale Modellierungsansatz mit dezentralen Anforderungen unterstützt diese Herangehensweise. Während sich der dezentrale Antragsteller inhaltlich verantwortlich zeichnet, ist das zentrale Administrationsteam für die technische Umsetzung zuständig.

Die klassischen Role-Engineering Verfahren bauen darauf, alle Anforderungen für eine Organisation zusammenzutragen und aus diesen Anforderungen schließlich über verschiedene Zwischenschritte ein RBAC-Modell zu erzeugen. Will man also einen systematischen Ansatz zur Rollenmodellierung verfolgen, so führt kein Weg an der zentralen Modellierung vorbei. Das trifft auf die Anwendungsseite zu, auf der eine Analyse erfolgen muss, welche Transaktionen mit welchen Berechtigungen möglich sein sollen, wie auch auf der Seite der Benutzergruppen, denen die Nutzung dieser Funktionen möglich gemacht werden soll. Beim dezentralen Ansatz ist der Verwalter der Einrichtung nicht nur mit den zu besetzenden Rollen und den damit verbundenen Implikationen überfordert, sondern auch mit der Struktur der Organisation aus RBAC-Sicht. Abhängig von der Tätigkeit an einer Hochschule hat eine Einrichtung eine eigene Sichtweise auf die Struktur der Universität. Bei der RBAC-Modellierung muss man sich schließlich auf ein Modell beschränken. Dieses kann dann für einen Teil der dezentralen Administratoren konsistent erscheinen, sicher aber nicht für alle, was zur Verwirrung führt. So herrschen faktisch evtl. ganz andere administrative Strukturen, als an zentraler Stelle geführt. Es gibt an der TU Berlin beispielsweise Labore oder Bibliotheken, die faktisch aus der Verwaltung ihrer übergeordneten Einheiten herausgelöst sind. Solchen Besonderheiten könnte durch eine zentrale Rollenadministration Rechnung getragen werden.

Im Fall der dezentralen Verwaltung wären die Administratoren auf die zentral vorgegebene Struktur angewiesen und müssten sich mit evtl. Jahrzehnte alten Vorgaben arrangieren. Grundsätzlich ist die von RBAC verwendete Rollenmetapher sehr gut dazu geeignet, die Rechteverwaltung beispielsweise für die eigene Einheit nachzuvollziehen oder sein Anliegen vorzubringen. Zwischen einer guten Metapher zur Verständigung mit den IT-Dienstleistern und der Übertragung der Administration auf einen Verantwortlichen in einer Einheit (z.B. einem Institut) gibt es jedoch noch diverse Zwischenformen, die eine zentrale Administration zulassen, wie z.B. das Formulieren von Anforderungen, die dann vom zentralen Rollenadministrationsteam umgesetzt wird.

3 Vorteile eines dezentral verwalteten Systems

In einem zentral verwalteten Identitätsmanagementsystem werden Rechtevergaben durch einen oder mehrere Administratoren vorgenommen. Leiter einer Organisationseinheit, die für ihre Mitarbeiter Zugang zu einer Anwendung benötigen, müssen sich dabei an den jeweils zuständigen Administrator wenden und eine Zugriffsgenehmigung erbitten. Im Gegensatz dazu verfolgt TUBIS einen dezentralen Ansatz der Rollenvergabe. Ein Leiter muss dabei nicht als Bittsteller gegenüber dem Anwendungsbetreiber auftreten, sondern kann die Rechte innerhalb seiner Organisationseinheit selbst verwalten. Dies führt mit der Zeit nicht zuletzt deshalb zu einer größer werdenden Akzeptanz des dezentralen Rollenverwaltungssystems, da etwaige Rechtfertigungen oder Begründungen für den Bedarf der Rechte entfallen. Die direkte Umsetzung der Rollenvergabe durch den jeweiligen Rollenverwalter führt zudem zu einer Minimierung der Bearbeitungszeit. In einem zentral verwalteten System erfolgt die Umsetzung der gewünschten Aktionen gewöhnlich nach dem FIFO Prinzip, was zu nicht transparenten Verzögerungen führen kann.

Dies wird noch verstärkt, wenn die Verfügbarkeit der Administratoren stark begrenzt ist. Die Rollenvergabe kann so schnell zum Flaschenhals werden. Im dezentralen System existiert dieser Engpass aufgrund der Verteilung nicht. Ist ein Rollenverwalter nicht verfügbar, so betrifft dies in erster Linie seine Organisationseinheit und beschränkt nicht die universitätsweite Arbeit. Durch die Integration von sogenannten Backuprollen wird dieser Flaschenhals noch weiter entschärft. Existiert in einer Organisationseinheit keine Person, der die Rolle des Rollenverwalters zugewiesen wurde, so erhält automatisch der Rollenverwalter der nächst höheren Organisationseinheit die Möglichkeit die darunter liegende Organisationseinheit mit zu verwalten. Sollte es in einer Organisationseinheit zwar einen Rollenverwalter geben, dieser allerdings kurzzeitig nicht verfügbar sein, so kann er seine Rolle als Rollenverwalter zuvor an jemand anderen delegieren, oder grundsätzlich in Vertretung geben. Im Fall der Vertretung erhält der Vertretende zwar die Zugriffsrechte als würde er selbst Mitglied der jeweiligen Rolle sein, agiert allerdings immer im Namen des ursprünglichen Rollenbesitzers. Vertretungen können dabei zeitlich begrenzt oder permanent vergeben werden. Dieser Gewinn an Selbstbestimmung ist einer der entscheidenden Vorteile des dezentralen Rollenverwaltungssystems. Der im Gegensatz dazu entstehende Arbeitsaufwand bleibt dabei gering und reduziert sich mit steigender Erfahrung mit dem System noch weiter.

Auf der Seite der Organisationseinheiten kann der zuständige Rollenverwalter Geschäftsrollen definieren. Dabei ist er völlig frei in der Anzahl und Benennung der Rollen. Eine Möglichkeit der Rollendefinition besteht darin, den Geschäftsverteilungsplan der Einheit als Rollen abzubilden. Jeder Geschäftsrolle kann der Rollenverwalter nun eine beliebige Auswahl der ihm zur Verfügung stehenden Anwendungsrollen zuweisen. Dadurch entsteht ein Grad an Flexibilität der durch ein zentral verwaltetes System faktisch nicht zu realisieren ist. Diese Umverteilung der Verantwortlichkeiten zur Rechtevergabe und damit auch Verschiebung der Arbeit, stieß zu Beginn der Einführung des dezentralen Rollenverwaltungssystems nicht immer auf Akzeptanz. In der Vergabe von Rechten wurde in erster Linie eine IT-Administration verstanden und weniger ein organisatorischer Verwaltungsprozess. Nicht selten wurde der IT-Dienstleister als Rollendienstleister verstanden. Nicht zuletzt die Definition der Rollendelegation als direkte Dienstanweisung führte hierbei zu einem allmählichen Umdenken. Dabei spielte insbesondere der Personalrat eine entscheidende Rolle, der neben der Anforderung einer automatischen Benachrichtigung eines Rollenempfängers über die Delegation oder den Entzug einer Rolle, die Delegation einer Rolle als Dienstanweisung verstanden wissen wollte. Hiermit soll unter anderem eine Aufgabenverteilung über die vertraglich geregelten Gebiete hinaus verhindert werden. Jedes Mitglied der TU kann sich über das persönliche Portal zudem im Rahmen der informationellen Selbstbestimmung alle seine im Rollenverwaltungssystem hinterlegten Daten anschauen. Dies beinhaltet auch alle ihm zugewiesenen Rollen inklusive der erhaltenen Vertretungen.

Auf der anderen Seite kann der Rollenverwalter einer Organisationseinheit jederzeit sehen, wer Mitglied seiner Geschäftsrollen ist. Dieses Maß an Transparenz ist, ergänzt durch die automatische Benachrichtigung einer Rollenzuweisung oder eines Rollenentzugs, ein Vorteil des dezentral verwalteten Systems.

Skepsis im Bezug auf die Verschiebung der Verantwortlichkeiten bei der Verwaltung von Zugriffsrechten von den jeweiligen Anwendungsadministratoren hin zu den Verantwortlichen der einzelnen Organisationseinheiten gab es nicht nur auf Seiten der Organisationseinheiten, sondern insbesondere auch auf Seiten der Anwendungsbetreiber. Dort führte die Verlagerung zu Verunsicherungen, da das Gefühl vorlag, dass sie damit die Kontrolle über ihre Anwendung zu einem entscheidenden Teil aus der Hand geben. Die Kontrollmöglichkeiten des Anwendungsbetreibers verlagern sich auf eine abstraktere Ebene. Der Anwendungsverwalter definiert seine verfügbaren Rechte und bündelt diese in Anwendungsrollen. Anschließend kann er entscheiden, welchem Nutzerkreis er diese Rollen zur Verfügung stellt. Dies kann sowohl eine bestimmte Organisationseinheit als auch eine Gruppe von Organisationseinheiten sein. Somit stellt er sicher, dass Rechte, die nur für einen bestimmten Typ von Organisationseinheit bestimmt sind, auch nur dort zur Verfügung stehen. Neben der strukturellen Zuordnung kann der Anwendungsbetreiber Anwendungsrollen auch so genanten Standardrollen zuweisen. Standardrollen sind Geschäftsrollen die sich aus bestimmten Tätigkeits- oder Statusgruppen, wie z.B. Hochschullehrer oder wissenschaftliche Mitarbeiter sowie den Studiengängen ableiten. Jede Person ist entweder durch ihren Vertrag oder durch die Immatrikulation einer Tätigkeitsgruppe oder einem Studiengang zugeordnet. Im Rollensystem werden die davon abgeleiteten Rollen automatisch den jeweiligen Personen zugewiesen. Der Anwendungsverwalter kann also festlegen, dass eine bestimmte Rolle z.B. allen Hochschullehrern oder allen Studierenden eines Studienganges zugewiesen werden soll. Darüber hinaus hat er aber keinen Einfluss auf konkrete Personalentscheidungen.

Nicht alle Anwendungsverwalter können sich mit dieser Art der Rechteverwaltung sofort anfreunden. In seltenen Fällen wurden Anwendungen nur deshalb in das Rollensystem integriert, weil dies durch die Leitung vorgegeben wurde. Nach erfolgreicher Integration der Anwendungen kam es aber auch bei den Anwendungsverwaltern zu einer wachsenden Akzeptanz der dezentralen Rechteverwaltung, da nach einem großen Aufwand zum Zeitpunkt der Integration, der Arbeitsaufwand in Bezug auf die Rechteverwaltung nach Einführung zurückgegangen ist. Die Integration neuer Anwendungen geschieht immer in Zusammenarbeit mit dem Rechenzentrum. Gemeinsam mit den Anwendungsbetreibern werden die Schnittstellen definiert. die Implementierung der Schnittstellen im Rollensystem und in der Authentisierungs- und Autorisierungsinfrastruktur werden vom Rechenzentrum durchgeführt. Eventuell notwendige Anpassungen an der Anwendung liegen in der Verantwortung des Anwendungsbetreibers. Mit der Integration in das IdM System der TU Berlin steht die neue Anwendung sofort den TU-Mitgliedern zur Verfügung. Diese Verteilung der Aufgaben auf mehrere Stellen führt insbesondere bei den Anwendungsbetreibern zu einer Verbesserung, da sich diese mehr der eigentlichen Pflege der Anwendung widmen können.

Ein weiterer Vorteil, der sich aus der Dezentralisierung der Rollenverwaltung ergeben hat, ist die flexible Realisierung von Nebenbedingungen (Constraints). Dabei können diese sowohl organisatorisch, als auch in der Implementierung, realisiert werden. Im System implementierte Regeln greifen sowohl in dezentralen als auch in zentralen Rollenverwaltungssystemen.

Organisatorisch realisierte Regeln sind im Allgemeinen auf bestimmte Organisationseinheiten begrenzt und nicht für die gesamte Universität gültig. Das Wissen über diese Regeln liegt daher in den jeweiligen Organisationseinheiten und nur selten an zentraler Stelle. Die Möglichkeit durch eine individuelle Rollenmodellierung bestimmte Constraints zu realisieren ist in der Vergangenheit als sehr positiv bewertet worden. Derzeit beschränkt sich die Modellierung von Constraints allerdings auf die bereits erwähnten Vertretungen von Rollen. Dabei kann jeder Rolleneigentümer seine Geschäftsrollen an eine andere Person in Vertretung geben. Neben der zeitlichen Begrenzung kann der Rolleneigentümer die Vertretung auf eine Auswahl der enthaltenen Zugriffsrechte beschränken. So kann ein Leiter einer Organisationseinheit seine Leiterrolle an mehrere Personen in Vertretung geben, die jeweils unterschiedliche Mengen der enthaltenen Rechte einschließen. In weiteren Schritten wird die Möglichkeit zur Definition von Nebenbedingungen noch weiter ausgebaut werden. Die Möglichkeit Nebenbedingungen lokal zu definieren, erhöht sowohl die Transparenz als auch die Flexibilität der Rechteverwaltung, was in dieser Form in einem zentral verwalteten System nicht möglich wäre.

Grundsätzlich lässt sich feststellen, dass die Skepsis dem Rollenverwaltungssystem gegenüber im Laufe der Zeit und mit steigender Erfahrung im Umgang mit dem System geringer geworden ist. Entscheidend dabei sind das Schulungsangebot und die Einrichtung eines Kundendienstes, der unterstützend zur Seite steht.

4 Schlussfolgerungen

Die Frage, ob der IT-Dienstleister auch die Funktion des Rollendienstleisters wahrnehmen soll, oder ob diese Aufgabe eher in die Verantwortung der jeweiligen Leiter der Organisationseinheiten gehört, müssen wir mit sowohl als auch beantworten. Grundsätzlich gehört die Spezifikation und Delegation von Geschäftsrollen in die Verantwortung des dezentralen Rollenverwalters, denn dort liegt das benötigte Know-how. Jeder muss nur den Teil des Rollenmodells verstehen, für den er auch die organisatorische Expertise besitzt. Der IT-Dienstleister muss dafür sorgen, dass er den Rollenverwaltern durch geeignete Werkzeuge, kombiniert mit einem umfangreichen Supportangebot, die bestmögliche Unterstützung bietet. Der Rollenverwalter, der die etablierten Prozesse und Aufgabenverteilungen kennt, kann die Zuordnung der benötigten Zugriffsberechtigungen an Geschäftsrollen vor Ort am besten vornehmen.

Die dezentralen Rollenverwalter haben die Möglichkeit mit den entsprechenden Werkzeugen ihr lokales Modell zu gestalten. Dabei können sie experimentieren und sofort auf die Ergebnisse reagieren, ohne jedes Mal mit einem zentralen Rollenexperten darüber zu diskutieren. Die eingesetzten Werkzeuge können diese Phase des Experimentierens unterstützen. An der TU-Berlin wurde hierzu das extrem RoleEngeneering (xRE) entwickelt [HKR08a]. Angelehnt an das Extrem Programming wird das Rollenmodell einer Organisationseinheit in mehreren Iterationen entwickelt. Der Rollenverwalter erhält dabei ein Feedback über Konflikte oder entstehende Redundanzen. Vor der Aktivierung des entwickelten Modells kann der Rollenverwalter dies in einer Sandbox testen.

Es ist einer der Grundgedanken des RBAC, die Verantwortung und Verwaltung von Rechten auf mehrere Schultern zu verteilen (Separation of Duty) [FCK95]. Dieser Grundgedanke kann sehr unterschiedlich implementiert werden. In TUBIS wird neben der organisatorischen Realisierung (Rechtespezifikation) auch die technische Realisierung (Rechtekonfiguration) den jeweils organisatorisch und rechtlich Verantwortlichen zugewiesen. Der Leiter einer Einrichtung ist befugt, seinen Mitarbeitern Aufgaben und die damit verbundenen Befugnisse zu delegieren. Es erscheint daher anmaßend, wenn eine Zentraleinrichtung in diesem Rahmen Entscheidungen in Frage stellt, oder gegenüber dem Leiter das Gefühl des Bittstellers vermittelt wird, oder er sich gar rechtfertigen muss. Die dezentralen Rollenverwalter stellen hohe Anforderungen an die Flexibilität im Bereich der Modellierung des eigenen Sub-Organigramms. TUBIS besitzt in dieser Hinsicht noch einige Schwächen und großes Ausbaupotential. Derzeit können die dezentralen Rollenverwalter beliebige Geschäftsrollen mit individuellen Namen erzeugen und mit den gewünschten Rechten ausstatten. Hier wird TUBIS um die Möglichkeit zur Definition von Nebenbedingungen erweitert. An dieser Stelle muss eine genaue Abwägung der Komplexität gemacht werden. Im ersten Schritt werden zwei Standard-Constraints realisiert werden: Zeitlich begrenzte Rollen sowie exklusive Rollen. Zeitlich begrenzte Rollen können sowohl über einen festen Zeitraum definiert werden, als auch nach bestimmten Regeln, z.B. nur montags, spezifiziert werden. Exklusive Rollen verbieten die Mitgliedschaft in einer bestimmten Kombination von Rollen. Entgegen des Bevormundungscharakters eines zentral verwalteten Systems verfolgte TUBIS das Ziel der Realisierung einer großen Gestaltungsfreiheit, deren Anfälligkeit gegenüber Fehlkonfigurationen durch geeignete Werkzeuge und Nebenbedingungen minimiert wird [Hil09].

Durch diese Selbstbestimmung ist der dezentrale Rollenverwalter nicht auf die Zuarbeit Dritter angewiesen. Dies bringt neben der Gestaltungsflexibilität auch eine große zeitliche Flexibilität. Der dezentrale Rollenverwalter kann immer sofort auf neue Anforderungen reagieren.

Auch im Bezug auf die Verfügbarkeit der Verwalter und des dadurch eventuell entstehenden Engpasses, bietet ein hybrides System eine optimale Lösung. Grundgedanke ist auch hier die Verteilung der Rollenverwaltung auf mehrere Schultern, damit eine Organisationseinheit durch Abwesendheit des Rollenverwalters oder einer Fehlkonfiguration zu keinem Zeitpunkt arbeitsunfähig werden kann. In diesem Fall existieren zusätzlich zentrale Rollenverwalter, die nach Antrag der betroffenen Organisationseinheit schnellst möglich die dezentrale Handlungsfähigkeit wieder herstellen. Kommt es in einem zentral verwalteten System zu einen solchem Problem, fehlt dabei die Fallback-Möglichkeit.

Transparenz spielt bei der Akzeptanz eines Systems eine entscheidende Rolle. Dabei zeigt sich, dass ein zentral verwaltetes System häufig Informationen auch nur in einer Form präsentiert, die für Außenstehende nur geringe Aussagekraft besitzt. Dem entgegen werden in einem System, dass hauptsächlich von nicht IT-Experten bedient wird, auch die Informationen in geeigneter Form präsentiert.

Die Verfügbarkeit neuer Anwendungen im Rollenverwaltungssystem ist hingegen eine Frage der Informationspolitik und unabhängig von der Wahl eines zentral oder dezentral verwalteten Systems. In beiden Systemen muss das Wissen über neue Anwendungen in die Organisationseinheiten gelangen. Um dieses Ziel zu erreichen, veranstaltet tubIT Informationsveranstaltungen zu neuen Anwendungen und Funktionen.

Weder ein zentral, noch ein dezentral verwaltetes System kann es schaffen die Wünsche aller Kunden zu erfüllen, da dies organisatorisch oder zum Teil auch technisch nicht möglich ist. Im Gegensatz zum zentral verwalteten System fördert das dezentral verwaltete System allerdings die Bereitschaft der Kunden an der Weiterentwicklung teilzunehmen.

5 Zusammenfassung

Aufgrund der Erfahrungen der letzten drei Jahre hat sich die Entscheidung für ein dezentral verwaltetes Identitätsmanagementsystem als geeignet erwiesen. Trotz der unvermeidlichen Kritik und dem anfänglich hohen Schulungsaufwand überwiegen inzwischen die Vorteile durch ein hohes Maß an Transparenz, Flexibilität und Selbstbestimmung. Der Großteil noch bestehender Defizite ist auf Fehler und Lücken der eingesetzten Werkzeuge zurückzuführen und nicht auf die Verlagerung der Verantwortung in die Organisationseinheiten hinein. Der Schwerpunkt der Weiterentwicklung wird daher auf der Verbesserung und Erweiterung der Methoden und Werkzeuge liegen. Mit der Entwicklung und Einführung des extreme RoleEngineering sind wir bereits einen entscheidenden Schritt in diese Richtung gegangen.

Literaturverzeichnis

[FCK95] D. F. Ferraiolo, J. A. Cugini, and D. R. Kuhn. Role-based access control (rbac): Features and motivations. *11th Annual Computer Security Application ...*, 1995.

[Hil09] T. Hildmann. Maßnahmen zum Schutz der Sicherheitspolitik bei der RBAC-Modellierung insbesondere bei der Verwendung von eXtreme Role-Engineering. In C. Paulsen, editor, *Sicherheit in vernetzten Systemen - 16. DFN Workshopband*. Books on Demand. Norderstedt, 2009.

[HKR08a] T. Hildmann, O. Kao, and C. Ritter. eXtreme Role Engineering: Ein neuer Ansatz zur Rechtedefinition und -vergabe. *GI Tagung Sicherheit 2008*, 2008.

[HKR08b] T. Hildmann, O. Kao, and C. Ritter. Rollenbasierte Identitäts- und Autorisierungsverwaltung an der TU Berlin. *1. DFN-Forum Kommunikationstechnologien Verteilte Systeme im Wissenschaftsbereich*, 2008.

[HR07] T. Hildmann and C. Ritter. TUBIS-Integration von Campusdiensten an der Technischen Universitat Berlin. *PIK-Praxis der Informationsverarbeitung und Kommunikation*, 30(3):145–151, 2007.

[SBCGY99] R. Sandhu, V. Bhamidipati, E. Coyne, S. Ganta, and C. Youman. The arbac97 model for role-based administration of roles. *ACM Transactions on Information and System Security*, 2:105–135, 1999.

[FKC07] D. F. Ferraiolo, D. R. Kuhn, and R. Chandramouli. *Role-Based Access Control*. Artec House, second edition, 2007.

Security

OpenID unter Sicherheitsgesichtspunkten

Tobias Dussa, KIT-CERT

tobias.dussa@kit.edu

Abstract: Der Authentifizierungsstandard OpenID ist im Web-2.0-Umfeld weit verbreitet. Ziel von OpenID ist es, dem Benutzer eine für alle OpenID unterstützenden Webseiten die gleiche Anmeldeprozedur zur Verfügung zu stellen, die zur Authentifizierung auf einen zentralen Dienst zugreift, so dass der Benutzer lediglich ein einziges Passwort verwalten muss. Dieser Beitrag beleuchtet den OpenID-Standard unter Sicherheitsgesichtspunkten und diskutiert insbesondere die Eignung als Authentifizierungsverfahren für andere Anwendungen als die klassischen Web-2.0-Plattformen.

1 Einleitung und Motivation

In den letzten Jahren sind im World Wide Web zahlreiche Dienste entstanden, die als »Web 2.0« zusammengefasst werden. Beispiele hierfür sind Blogs, Wikis, Webmaildienste und Plattformen für soziale Netzwerke. Ihnen gemeinsam ist, dass sie nicht nur statische, für alle Benutzer gleiche Inhalte anbieten, sondern auch individuelle, an den einzelnen Benutzer angepasste Mehrwerte erbringen. Hierfür ist es Voraussetzung, einerseits die verschiedenen Benutzer voneinander unterscheiden, andererseits deren Daten voneinander trennen und den Zugriff darauf kontrollieren zu können. Es ist also nötig, den einzelnen Benutzer zu identifizieren und zu authentifizieren.

Das für Webdienste klassische Verfahren, Benutzer zu authentifizieren, ist die traditionelle Abfrage von Benutzername und zugehörigem Passwort. Benutzer können typischerweise ohne weiteres Zutun des Betreibers eigene Konten anlegen und verwalten.

Während dieser Ansatz zur Authentifizierung für den Betreiber eines Webdienstes vorteilhaft ist, weil er sich leicht implementieren lässt und dem Betreiber die Kontrolle über die Authentifizierungsdaten der Benutzerkonten belässt, bringt er den Benutzer rasch an seine Grenzen. Da ein Benutzerkonto in der Regel nur für einen Webdienst gültig ist, muss der Anwender für jeden Webdienst ein neues Konto einzurichten. Im Idealfall kann dabei derselbe Benutzername verwendet werden, dies ist aber wegen potentiell verschiedener Vorschriften für gültige Benutzernamen einerseits, Kollisionen von Benutzernamen andererseits nicht selbstverständlich. Hinzu kommt, dass für jedes Konto üblicherweise auch ein Passwort gewählt werden muss. Der Benutzer ist damit ohne technische Hilfsmittel vor die Wahl gestellt, entweder ein Passwort für mehrere Konten zu verwenden oder zu verfolgen, welches Passwort für welchen Webdienst gilt. Beides ist wenig wünschenswert, so dass sich in der Praxis verschiedene Hilfsmittel etabliert haben, die dem Benutzer die Verwaltung seiner Zugangsdaten erleichtern. Ein bekanntes Beispiel ist die Passwortablage

des Mozilla Firefox, die für gegebene URLs den gültigen Benutzernamen und das dazugehörige Passwort speichert.[Cot] Solche Hilfsmittel bergen auch Nachteile; geht etwa die Passwortablage verloren, so sind damit auch sämtliche damit verwalteten Zugangsdaten nicht mehr verfügbar.

OpenID versucht, diesen Problemen zu begegnen, indem eine global gültige und eindeutige Benutzerkennung eingeführt wird. Es ist für den Benutzer weiterhin nötig, bei jedem Webdienst ein separates Konto anzulegen; hingegen wird die Authentifizierung auf einen einzigen Webdienst konzentriert. Auf diese Weise können einige oben beschriebene Nachteile umgangen werden:

- Die Vielzahl verschiedener Benutzerkennungen wird im Regelfall auf eine einzige OpenID-Benutzerkennung reduziert.
- Durch die Bündelung der Authentifizierung reduziert sich die Anzahl der Passwörter; der Benutzer muss sich nur ein einziges Passwort merken.
- Die Dienstanbieter haben keinen Zugriff mehr auf Authentifizierungsdaten der Benutzer, wodurch der mögliche Schaden bei Fehlverhalten schrumpft.

Während OpenID aus Benutzersicht also einige Vorteile gegenüber den klassischen Anmeldemethoden bietet, birgt das Verfahren bei genauerer Betrachtung sowie aus Sicht eines Dienstanbieters auch Schwachstellen. Diese Perspektive wird etwa dann relevant, wenn der Zugang zu wertvollen Ressourcen, beispielsweise klassischen Rechenressourcen, geschützt werden soll. Entsprechende Ansätze sind etwa in Cloud-Computing-Projekten zu finden, wenn der eigentliche Zugriff auf die Ressourcen zwar mittels SSH durchgeführt, der Zugriff auf die zentrale Verwaltung von Benutzerkonten aber mit Hilfe von OpenID gesichert wird; als konkretes Beispiel sei das OpenCirrus-Projekt genannt, in dem das beschriebene Vorgehen vorgeschlagen und diskutiert wurde.[DKM09]

Nachfolgend werden zunächst verwandte Arbeiten aufgezeigt, um danach die Funktionsweise des OpenID-Protokolls näher zu erläutern. Im nächsten Abschnitt werden daraus resultierende Schwachstellen von OpenID beschrieben. Im fünften Abschnitt werden die vorgestellten Schwachstellen bewertet; der sechste Abschnitt beinhaltet schließlich eine Zusammenfassung und Möglichkeiten des weiteren Vorgehens.

2 Weitere Arbeiten

Die Sicherheitsaspekte von OpenID werden teilweise in Version 2.0 der Spezifikation des OpenID-Standards zur Authentifizierung diskutiert.[FRHH07] Schwerpunkt dieser Diskussion sind Sicherheitsprobleme aus Sicht des Anwenders. Einige Gesichtspunkte werden weiterhin in der Spezifikation der OpenID-Erweiterung “OpenID Provider Authentication Policy Extension 1.0” betrachtet.[RJS08] Zusätzlich stellen die Entwickler von OpenID eine Wikiseite mit Empfehlungen für den sicheren Einsatz bereit.[ART09]

Schließlich stellen Eugene und Vlad Tsyrklevich in ihrem Vortrag “Single Sign-On for the Internet: A Security Story” sowie ihrem Whitepaper weitere Probleme vor.[TT07a, TT07b]

3 Funktionsweise des OpenID-Protokolls

In diesem Abschnitt wird der Ablauf einer Authentifizierung nach OpenID-Standard Version 2.0 zunächst kurz umrissen, dann etwas detaillierter dargestellt.[FRHH07]

Beim OpenID-Authentifizierungsprotokoll sind mehrere Parteien beteiligt:

- Der Benutzer (Alice), der sich bei einem Webdienst anmelden möchte.
- Der Webdienst (Bob), bei dem sich der Benutzer anmelden möchte. Im OpenID-Jargon wird dieser Webdienst auch als "Relying Party" oder "RP" bezeichnet.
- Den OpenID Provider (Trent), dem gegenüber sich der Benutzer authentifiziert. In OpenID-Terminologie wird der OpenID Provider auch als "OP" bezeichnet.

Eine Authentifizierung nach OpenID läuft im wesentlichen in den folgenden Schritten ab:

1. Alice gibt gegenüber Bob einen "User-Supplied Identifier" an, vergleichbar mit einem Accountnamen. Dieser Identifier ist im wesentlichen ein URL oder ein XRI (Extensible Resource Identifier, siehe [RM05]).
2. Bob führt den sogenannten "Discovery Process" mit dem im übergebenen Identifier durch. Dadurch wird der URL des OpenID-Providers, also Trent, ermittelt.
3. Optional führt Bob mit Trent eine sogenannte Association mit Schlüsselaustausch durch, um die weitere Kommunikation zwischen Bob und Trent abzusichern.
4. Bob leitet Alice mittels eines HTTP-Redirects oder eines HTTP-Posts zu Trent um; dieser Schritt wird als "Authentication Request" bezeichnet.
5. Alice authentifiziert sich gegenüber Trent.
6. Trent leitet Alice mit einem weiteren HTTP-Redirect oder -Post zurück zu Bob und übergibt darin Informationen über Alices Authenfizierungszustand an Bob.
7. Bob prüft die übergebenen Informationen zum Authentifizierungszustand von Alice.

Bei einigen Protokollschritten sind nähere Details für die spätere Diskussion wichtig. Aus diesem Grund werden im Folgenden die einzelnen Schritte näher beschrieben.

3.1 Die Identifizierung des Benutzers

Die Authentifizierung wird vom Benutzer, also Alice, initiiert. Alice identifiziert sich gegenüber Bob, gibt also eine OpenID-Identität an, die sie zu besitzen behauptet. Dies kann etwa wie bei klassischen Mechanismen durch ein einfaches Webformular geschehen.

3.2 Der Discovery Process

Beim Discovery Process ermittelt Bob mit Hilfe des User-Supplied Identifiers von Alice den für sie zustandigen OpenIP-Provider, also Trent. Identifier können als URL oder als XRI angegeben werden; ihre Verarbeitung hängt vom verwendeten Format ab.

Handelt es sich beim User-Supplied Identifier um einen XRI, so wird dieser nach den Umwandlungsregeln in [WRC+06] in eine Extensible Resource Descriptor Sequence (XRDS, ebenfalls in [WRC+06]) umgewandelt, die direkt die benötigten Informationen enthält.

Handelt es sich dagegen um einen URL, so soll erst mittels Yadis-Protokoll (siehe [Mil06]) versucht werden, den URL in eine XRDS umzuwandeln. Gelingt dies nicht, so wird der URL heruntergeladen; danach soll ein HTML-basierter Discovery-Prozess durchgeführt werden. Gemäß OpenID-Spezifikation muss der HTML-basierte Discovery-Prozess von der Relying Party, also Bob, unterstützt werden.

Gelingt die Discovery, so weiß Bob, welcher OP, also Trent, für Alice zuständig ist.

3.3 Die Association

Zwischen Bob und Trent kann eine sogenannte Association durchgeführt werden. Während der Assoziierung wird mit einem Diffie-Hellman-Schlüsselaustauschs ein gemeinsames Geheimnis etabliert, mit dem die weitere Kommunikation zwischen diesen Partnern abgesichert werden kann.[Res99]

Gelingt eine Assoziierung nicht, beispielsweise weil Trent dies nicht unterstützt, so kann Bob im Protokoll fortfahren oder die Authentifizierung abbrechen.

3.4 Der Authentication Request

In diesem Protokollschritt beantragt Bob bei Trent die Authentifizierung von Alice. Dieser Antrag wird in Form indirekter Kommunikation gestellt: Bob schickt einen HTTP-Redirect oder einen HTTP-Post an Alice, der Alices Anwendung – etwa ein Webbrowser – an den ermittelten OP, also Trent, weiterleitet. Alice' Client initiiert daraufhin die Authentifizierung gegenüber Trent. In der Weiterleitung werden von Bob einige Parameter der beantragten Authentifizierung an Trent übergeben.

3.5 Die Authentifizierung

Alice authentifiziert sich gegenüber Trent. Der OpenID-Standard spezifiziert diesen Schritt nicht näher, da die Authentifizierung in Trents Verantwortungsbereich fällt.

Falls in der Authentifizierungsanfrage eine Assoziierung zwischen Bob und Trent referen-

ziert wurde, so soll Trent speichern, dass für diese Assoziierung eine Authentifizierung durchgeführt wurde, um ein Wiederverwenden der Assoziierung zu verhindern. Wurde keine Assoziierung übergeben, so muss Trent eine »einseitige Assoziierung« generieren und zum Zwecke der späteren Verifikation speichern.

3.6 Die Authentication Response

Nach erfolgter Authentifizierung leitet Trent Alice' Browser wieder mittels eines HTTP-Redirects oder -Posts zurück zu Bob. Analog zum Authentifizierungsantrag werden auch hier wieder einige Details zur Authentifizierung übertragen; insbesondere müssen eine eindeutige Transaktionsnummer ("Nonce"), die verwendete Assoziierung sowie eine digitale Signatur angegeben sein.

3.7 Die Prüfung der Authentifizierung

Nachdem Alice wieder zurück zu Bob verwiesen wurde, verifiziert Bob die von Trent indirekt übergebene Nachricht. Einige Angaben müssen gemäß OpenID-Standard geprüft werden, unter anderem der verwendete URL der Weiterleitung von Trent zu Bob, die enthaltenen Angaben zur Identität von Alice, Trents Transaktionsnummer sowie die Signatur.

Die Angaben zur Identität von Alice können nur insofern geprüft werden, als dass sie zu Alice' Angaben im ersten Protokollschritt passen. Trents Transaktionsnummer wird dahingehend geprüft, dass sie nicht für eine vorherige Authentifizierung verwendet wurde.

Zur Prüfung der Signatur ist eine Fallunterscheidung nötig. Liegt eine Assoziierung zwischen Bob und Trent vor, so besteht ein gemeinsames Geheimnis, mit dem Bob direkt die Signatur verifizieren kann. Wurde keine Assoziierung durchgeführt, kann Bob die Signatur nicht überprüfen, da ihm der verwendete Signaturschlüssel nicht bekannt ist. In diesem Fall muss Bob bei Trent prüfen, ob die angegebene Signatur gültig ist. In der Anfrage schickt Bob alle signierten Daten sowie die Signatur selber an Trent, der dann entscheidet, ob es sich um eine legitime Signatur handelt; aus diesem Grund muss Trent im Authentifizierungsschritt die einseitig generierte Assoziierung speichern (siehe Abschnitt 3.5).

4 Beschreibung erkannter Schwachstellen

Das OpenID-Authentifizierungsprotokoll weist einige Angriffspunkte auf, die im Folgenden beschrieben werden.

4.1 Klassische Netzwerkangriffe

Dieser Abschnitt geht auf einige klassische Angriffe auf Kommunikationsprotokolle: Mitlesen und Verändern von Inhalten, Man-in-the-Middle- und Replay-Attacken.

Die OpenID-Authentifizierung ist zunächst nicht besonders gegen Mitlesen gesichert. Damit sind zwar keine Authentifizierungsdaten von Benutzern gefährdet – die eigentliche Authentifizierung erfolgt außerhalb der OpenID-Spezifikation gegenüber Trent –, es kann aber durchaus festgestellt werden, welcher Benutzer sich wann gegenüber welchen Webdiensten authentifiziert.

Replay-Attacken, in denen der Angreifer durch erneutes Versenden mitgeschnittener Pakete Vorteile erlangt, sind zwar durch die Verwendung von Nonces in den Nachrichten von Trent an Bob ausgeschlossen, da damit sichergestellt wird, dass die Meldung einer erfolgreichen Authentifizierung nur ein Mal verwendet werden kann. Dies setzt allerdings voraus, dass Alice als erste Bob gegenüber Trents Bestätigung ihrer Authentifizierung präsentiert. Ist ein Angreifer in der Lage, Trents Antwort mitzulesen und schneller zu Bob weiterzuleiten als Alice, so kann er Alices Authentifizierung übernehmen.

Gegen das Verändern von Inhalten bietet OpenID nur teilweise Schutz; insbesondere bei der Rückmeldung von Trent an Bob sind die wesentlichen Teile der Nachricht digital signiert und können nicht ohne weiteres unbemerkt verändert werden. Es ist bis zu diesem Protokollschritt aber möglich, Inhalte unbemerkt zu modifizieren; damit kann sich ein Angreifer als Trent ausgeben, wenn er geschickt die relevanten URLs verändert. Auf diese Weise können etwa Alices Authentifizierungsdaten ausgespäht werden.

Auch Man-in-the-Middle-Attacken sind möglich. Ein Angreifer, der sich in Protokollschritt 3, der Assoziierung, zwischen Bob und Trent setzen kann, ist in der Lage, den Diffie-Hellman-Schlüsselaustausch zu unterlaufen. Er kann danach gegenüber Bob als Alice aufzutreten, indem er korrekt signierte Antwortnachrichten herstellt, und so als Alice auftreten, ohne ihre Authentifizierungsdaten kennen zu müssen.

4.2 Besondere Risiken für Benutzer

Zusätzlich zu den Risiken, die von klassischen Angriffen ausgehen, ist OpenID noch gegenüber anderen Gefahren verwundbar.

Ziel des OpenID-Standards ist es, dem Benutzer die Verwaltung einer Vielzahl verschiedener Benutzerkonten zu ersparen, indem ein einziger OpenID-Identifier bei allen teilnehmenden Webdiensten zur Identifizierung und Authentifizierung verwendet wird. Die Authentifizierung erfolgt gegenüber einem einzigen OpenID-Provider, was dem Benutzer das Leben erleichtert, aber auch Risiken birgt.

Sämtliche Anmeldevorgänge eines Benutzers gegenüber Webdiensten werden an einen zentralen OP weitergeleitet. Der OP ist damit in der Lage, das Benutzerverhalten zu protokollieren und zu profilieren. Da Anmeldungen je nach Implementierung seitens des OP auch ohne Benutzerinteraktion erfolgen können – etwa mit Hilfe von zeitlich begrenzt

gültigen Cookies –, kann unbemerkt ein detailliertes Bild der aufgerufenen Webdienste erstellt werden.

Ist eine Single-Sign-On-Funktionalität wie eben umrissen implementiert, so eröffnen sich einem Angreifer noch schwerwiegendere Angriffsmöglichkeiten. Hat ein Benutzer eine erfolgreiche Authentifizierung durchlaufen, so kann ein Angreifer vom Benutzer nicht beabsichtigte Aktionen bei Webdiensten auslösen, indem er den Webbrowser des Benutzer dazu bringt, einen entsprechenden URL zu laden.

Zudem spricht der Benutzer durch die Verwendung von OpenID dem OP implizit besonderes Vertrauen aus, denn der OP ist jederzeit in der Lage, sich gegenüber einem OpenID-Dienst als Benutzer auszugeben. Dies impliziert eine besondere Verantwortung des OP im Sinne eines sicheren Betriebs, aber auch die Erwartung eines besonders korrekten eigenen Handelns.

4.3 Besondere Risiken für Dienstanbieter

Im vorigen Abschnitt wurden die Gefahren aus Nutzersicht betrachtet. Aus Sicht eines Dienstbetreibers ergeben sich weitere Schwierigkeiten.

Für den einzelnen Benutzer stellt der für ihn zuständige OP eine Authentifizierungsbündelung dar. Der OP ist die einzige Stelle, der gegenüber der Benutzer sich authentifiziert. Im Extremfall kann der Benutzer sogar seinen eigenen OP betreiben so dass er die vollständige Kontrolle über seine Anmeldedaten behält.

Für einen Dienstanbieter – Bob – ist dieses Konzept keine Zentralisierung, sondern eine Dezentralisierung. Bob ist zur Authentifizierung auf den vom Benutzer angegebenen OP angewiesen. Insbesondere weiß Bob nichts darüber, welche Güte die Authentifizierung eines gegebenen OPs hat. Folglich muss Bob im Zweifel davon ausgehen, dass eine OpenID-Authentifizierung praktisch wertlos ist.

Zusätzlich birgt das OpenID-Protokoll noch grundsätzlichere Probleme für den Dienstanbieter. Gibt Alice einen Identifier in URL-Form an, so ist Bob gezwungen, diesen URL herunterzuladen, solange er mit `http://` oder `https://` beginnt – in Version 1.1 des OpenID-Standards gab es gar keine Einschränkungen, so dass etwa URLs der Form `file://` gültig[RF06] waren. Damit sind Denial-of-Service-Angriffe trivial durchführbar, indem ein Angreifer einen URL angibt, der eine große Datenmenge referenziert. Auch Portscans anderer Maschinen sind denkbar; diese Scans gehen dann von Bob aus und führen nicht unmittelbar zum eigentlichen Angreifer.

Schließlich ist zu bemerken, dass der Alice sich gegenüber Bob authentifiziert, indem sie auf einen OP verweist, der Bob bestätigt, dass Alice tatsächlich Alice ist. Dieser OP steht in keinem definierten vorherigen Vertrauensverhältnis zu Bob und kann beliebige Informationen zurückliefern.

5 Bewertung der Schwachstellen

Die Tragweite der im obigen Abschnitt diskutierten Schwachstellen ist abhängig von den Umständen, unter denen OpenID eingesetzt werden soll.

Die in Abschnitt 4.1 beschriebenen Angriffe sind nicht spezifisch für OpenID. Ihnen kann in der Regel leicht und wirkungsvoll etwa durch den Einsatz von SSL begegnet werden. Diesem Umstand wird auch im OpenID-Standard Rechnung getragen, indem empfohlen wird, SSL einzusetzen. Dies ist insofern bemerkenswert, als dass damit der Diffie-Hellman-Schlüsselaustausch obsolet wird, da er dann nichts zur Sicherheit beiträgt.

Wird auf die Absicherung mittels SSL verzichtet, so ist praktisch der gesamte Authentifizierungsvorgang nicht nur gegenüber Mitlesen, sondern auch gegenüber einem breiten Spektrum an netzwerkbasierten Angriffen verwundbar. Ein Angreifer kann beispielsweise die Identität eines Opfers annehmen, indem er eine erfolgreiche Authentifizierung abfängt und selber verwendet, oder die Authentifizierungsdaten eines Opfers ausspähen, indem er die Weiterleitungen zum OpenID-Provider abfängt, das Opfer zu sich selber weiterleitet und vorgibt, der fragliche OP zu sein. Es ist daher praktisch unerlässlich, durchgängig SSL zur Sicherung der Übertragung einzusetzen.

Die in Abschnitt 4.2 diskutierten Risiken für den Anwender sind teilweise erheblich, hängen aber davon ab, in welchem Umfang OpenID eingesetzt wird. Je mehr ein Benutzer von OpenID Gebrauch macht, desto genauer wird das Profil, das der OP erstellen kann.

Aus Betreibersicht stellt sich der Einsatz von OpenID gerade im Hochschulumfeld je nach genauem Einsatzzweck als problematisch heraus. Unkritisch ist die Verwendung nur dann, wenn die damit geschützten Inhalte keinen besonderen Wert für den Betreiber einerseits, aber auch keine besonderen persönlichen Daten der Benutzer andererseits umfassen. Im allgemeinen besteht kein Anlass für den Betreiber, einem beliebigen OpenID-Provider besonderes Vertrauen entgegenzubringen. Eine Authentifizierung ist daher ohne weitere Rahmenbedingungen nicht aussagekräftig, zumal im Zweifel ein Benutzer seinen eigenen OP betreiben kann. Der Zugriff auf wertvolle Ressourcen, etwa einen Höchstleistungsrechner, sollte daher nicht ohne weiteres auf der Authentifizierung mittels OpenID beruhen. Allerdings kann hier Abhilfe geschaffen werden, indem nicht beliebige OPs, sondern nur tatsächlich vertrauenswürdige OPs – etwa alle von Hochschulen betriebenen OPs – akzeptiert werden. Allerdings hebelt diese Einschränkung das Ziel von OpenID, dass jeder Anwender nur eine einzige Identität benötigt, teilweise aus. Hier ist die 2008 spezifizierte “OpenID Provider Authentication Policy Extension 1.0” bemerkenswert.[RJS08] Diese Spezifikation soll es ermöglichen, die Güte einer Authentifizierung zu messen, indem der OP dem Dienstanbieter Informationen über seine Authentifizierungsverfahren zur Verfügung stellt. Dies ändert aber offensichtlich nichts am grundsätzlichen Problem, dass der Dienstanbieter den Aussagen des OP blind glauben muss. Hier handelt es sich um eine konzeptionelle Schwäche von OpenID, die nicht ohne weiteres behoben werden kann.

Noch eindeutiger wird die Lage, wenn sensible Bereiche persönlicher Informationen berührt werden. Dies ist beispielsweise dann der Fall, wenn der Zugang zu Studienportalen mittels OpenID geregelt würde. In derartigen Portalen können Studierende typischerweise Einblick in ihre Studienleistungen nehmen, sich zu Prüfungen an- und abmelden oder sich

sogar zurückmelden oder exmatrikulieren. Wird hier ohne weitere Einschränkung OpenID zur Authentifizierung verwendet, würde jedes der oben beschriebenen Sicherheitsprobleme dazu führen, dass unberechtigt Zugriff auf diese Daten genommen werden könnte. Die Hochschule hat hier schon aus rechtlichen Gründen für einen hinreichenden Schutz derartig sensibler Daten zu sorgen, der mit OpenID sicher nicht ohne weiteres gegeben ist.

Für Anwendungen, die nicht derartig hohe Bedürfnisse an die Sicherheit haben, ist OpenID dagegen gut zur Authentifizierung geeignet. Dieser Umstand spiegelt das Umfeld wider, für das OpenID ursprünglich konzipiert war: OpenID soll einen Ersatz für die klassische Benutzername-Passwort-Authentifizierung für Web-2.0-Dienste bieten. Diese Dienste haben in der Regel sehr geringe Sicherheitsanforderungen. Ein Benutzerkonto kann häufig durch den Benutzer selber angelegt und aktiviert werden; die Angaben des Benutzers werden in der Regel nicht oder nur oberflächlich geprüft. Gemessen an diesen Sicherheitsstandards ist OpenID in der Tat eine attraktive Alternative, weil sie dem Benutzer den Umgang mit einer Vielzahl von Web-2.0-Diensten erleichtert, ohne wesentliche Einbußen in der Sicherheit mit sich zu bringen.

Für Dienstbetreiber mit höheren Sicherheitsanforderungen ist OpenID nur dann eine Option, wenn es einerseits zwingend mit SSL abgesichert wird, um den klassischen Netzwerkangriffen wirkungsvoll entgegenzutreten, und andererseits nur als vertrauenswürdig bekannte OpenID-Provider zugelassen werden, da ansonsten die Authentifizierung praktisch wertlos ist. Da aber gerade die Freiheit der Wahl des OpenID-Providers ein zentrales Merkmal von OpenID ist, scheint es damit fraglich, ob nicht die Verwendung anderer Verfahren, etwa Shibboleth, einen ähnlichen Komfortgewinn für den Benutzer bringen würde, ohne dieselben Schwachstellen wie OpenID aufzuweisen.

6 Zusammenfassung und Ausblick

In diesem Artikel wurde das OpenID-Authentifizierungsverfahren vorgestellt und dessen Sicherheitsschwachstellen diskutiert. Neben klassischen Angriffen, denen vergleichsweise einfach durch den Einsatz von SSL abgeholfen werden kann, birgt OpenID aufgrund seiner Architektur weitere Schwachstellen. Die Bündelung aller Authentifizierungsvorgänge eines Benutzers bei einem OpenID-Providers gewährt diesem Zugriff auf eine Vielzahl sensibler Daten. Ist zudem eine Single-Sign-On-Funktionalität implementiert, so kann durch einen Angriff auf den Browser eines Anwenders Zugriff auf sämtliche OpenID unterstützenden Webdienste erlangt werden.

OpenID bietet für den Anwender die Chance, die Authentifizierung zu vereinheitlichen und in der Handhabung zu vereinfachen, aber auch sicherer zu gestalten. Aus Betreibersicht müssen zusätzliche Maßnahmen zur Absicherung in Betracht gezogen werden, so dass der Einsatz von OpenID möglicherweise nicht sinnvoll ist. Zudem muss berücksichtigt werden, dass einige Schwachstellen protokollbedingt nicht behebbar sind.

Für die weitere Entwicklung erscheinen zwei Bereiche besonders interessant. Derzeit sind gerade aus Sicht von Dienstanbietern mit höheren Sicherheitsanforderungen noch einige Probleme offen; hier ist mit der “OpenID Provider Authentication Policy Extension 1.0”

bereits ein erster Schritt getan, der weiter ausgebaut werden könnte.

Zweitens bietet OpenID Angriffspunkte, die es einem Angreifer erlauben, einen OpenID unterstützenden Dienstanbieter in begrenztem Maße als Proxy für Attacken auf weitere Systeme zu missbrauchen oder sehr leicht eine Denial-of-Service-Attacke gegen den Webdienst selbst auszuführen. Hier liegt weiteres Entwicklungspotential.

Literatur

[ART09] Andrew Arnott, David Recordon und Allen Tom. OpenID Security Best Practices. Seite im OpenID-Wiki, Juni 2009. http://wiki.openid.net/OpenID-Security-Best-Practices, aufgerufen am 18. November 2009, letze Änderung am 8. Juni 2009.

[Cot] Sean Cotter. PSM 2.1 & Privacy Help: Status and Work in Progress. Webseite. http://www.mozilla.org/projects/security/pki/psm/help_21.

[DKM09] Tobias Dussa, Michael Kozouch und Dejan Milojicic. Open Cirrus Global Sign-On. Technical report, OpenCirrus Project, Mai 2009.

[FRHH07] Brad Fitzpatrick, David Recordon, Dick Hardt und Josh Hoyt. OpenID Authentication 2.0 — Final. Spezifikation, Dezember 2007. http://openid.net/specs/openid-authentication-2_0.txt.

[Mil06] Joaquin Miller. Yadis Specification Version 1.0. Spezifikation, März 2006. http://yadis.org/papers/yadis-v1.0.pdf.

[Res99] Eric Rescorla. Diffie-Hellman Key Agreement Method. Request for Comments, Juni 1999. http://www.faqs.org/rfcs/rfc2631.txt.

[RF06] David Recordon und Brad Fitzpatrick. OpenID Authentication 1.1. Spezifikation, Mai 2006. http://openid.net/specs/openid-authentication-1_1.txt.

[RJS08] David Recordon, Michael B. Jones und Nat Sakimura. OpenID Provider Authentication Policy Extension 1.0. Spezifikation, Dezember 2008. http://openid.net/specs/openid-provider-authentication-policy-extension-1_0.txt.

[RM05] Drummond Reed und Dave McAlpin. Extensible Resource Identifier (XRI) Syntax V2.0. Spezifikation, November 2005. http://www.oasis-open.org/committees/download.php/15376.

[TT07a] Eugene Tsyrklevich und Vlad Tsyrklevich. Single Sign-On for the Internet: A Security Story. Vortrag auf der Konferenz “Black Hat Las Vegas 2007”, August 2007. http://www.blackhat.com/presentations/bh-usa-07/Tsyrklevich/Presentation/bh-usa-07-tsyrklevich.pdf.

[TT07b] Eugene Tsyrklevich und Vlad Tsyrklevich. Single Sign-On for the Internet: A Security Story. Whitepaper zum Vortrag auf der Konferenz “Black Hat Las Vegas 2007”, August 2007. https://www.blackhat.com/presentations/bh-usa-07/Tsyrklevich/Whitepaper/bh-usa-07-tsyrklevich-WP.pdf.

[WRC+06] Gabe Wachob, Drummond Reed, Les Chasen, William Tan und Steve Churchill. Extensible Resource Identifier (XRI) Resolution V2.0. Arbeitsentwurf 10, März 2006. http://www.oasis-open.org/committees/download.php/17293.

GSM für die Lehre – Basisstation, IMSI-Catcher und Monitordevices aus Standardkomponenten selbst gebaut

Dirk von Suchodoletz, Dennis Wehrle, Holger Bertsch

dirk.von.suchodoletz@rz.uni-freiburg.de
dennis.wehrle@rz.uni-freiburg.de
holger.bertsch@gmx.de

Lehrstuhl für Kommunikationssysteme
Rechenzentrum der Universität Freiburg
Hermann-Herder-Str. 10
79104 Freiburg

Abstract: Für Demonstrationszwecke in Vorlesungen und für Sicherheitsuntersuchungen ist der Aufbau einer prototypischen GSM Base Tranceiver Station von Interesse. Ähnlich wie für Lehrveranstaltungen zu Netzwerken, die sinnvollerweise vielseitige praktische Demonstrationen bieten, sollte dieses auch für den Bereich Mobilfunk gelten. Durch den Betrieb einer eigenen BTS können viele Abläufe auf verschiedenen Layern analysiert und nachvollziehbar gemacht werden. Darüber hinaus lassen sich bestehende Sicherheitslücken gut mit Hilfe eines IMSI-Catchers illustrieren. Diesbezüglich wird gezeigt, wie Mobilfunkteilnehmer sich ohne ihr Wissen in den IMSI-Catcher einbuchen und überwacht werden können, ohne dass ihnen ihr Mobiltelefon das mitteilt. Die Kontrolle, der sie hierbei unterliegen, beinhaltet, abgesehen vom Auslesen der IMSI und IMEI, auch eine Auflistung aller aktuell geführten Gespräche und die Möglichkeit diese aufzuzeichnen.

1 Einleitung

Die Black-Box-Ära im Mobilfunk neigt sich ihrem Ende entgegen. Neue Hardwareentwicklungswerkzeuge und Open-Source-Mobilfunklösungen öffnen das Feld für den informierten Jedermann. Mobilfunknetze haben die heutige Lebenswelt komplett durchdrungen. Die mobile Telekommunikationslandschaft hat sich in den letzten 20 Jahren signifikant demokratisiert. Verfügte früher eine sehr überschaubare Elite aus Politik und Wirtschaft über die Technik in gewissem Rahmen mobil zu telefonieren, so ist die Zahl der registrierten SIMs in Deutschland höher als die der Einwohner. Weltweit nutzen mehr als zwei Milliarden Menschen GSM. Bisher fanden Sicherheitsdiskussionen und mögliche Angriffsszenarien auf diese Infrastruktur nur in kleinen Fachzirkeln statt. Die neuen Möglichkeiten werden diesen Zustand in den nächsten Jahren sicherlich verändern und neue Sicherheitsdiskussionen hervorrufen [PN09].
Dieses schafft zudem ganz neue Grundlagen, um aus rein theoretischen Vorlesungen zum

Thema eine deutlich interaktivere Veranstaltung mit praktischen Demonstrationselementen zum Nachbauen und Analysieren zu machen. Damit lassen sich aktuelle GSM-Infrastrukturen ähnlich gut präsentieren, wie diverse Internet-Protokolle.

2 Die selbstgebaute GSM-Zelle

Zum Aufbau eines kleinen GSM-Mobilfunknetzes muss nicht komplett die mehrtausendseitige Spezifikation umgesetzt werden. Es genügen die zentralen Komponenten des Radio und des Network Subsystems, um mit herkömmlichen Mobiltelefonen bereits Gespräche führen zu können oder SMS zu empfangen. Die Base Transceiver Station einer kleinen Zelle mit bis zu sieben Teilnehmern lässt sich mittels eines Universal Software Radio Peripheral (USRP) an einem Steuercomputer betreiben. Eine Übersicht und einen Vergleich zwischen der GSM-Infrastruktur und dem Setup mittels USRP gibt die Abbildung 1.

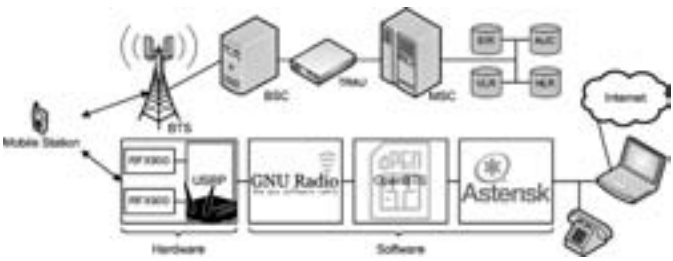


Abbildung 1: Systemüberblick der benötigten Hard- und Softwarekomponenten für den Aufbau einer kleinen GSM-Zelle.

Das von der Firma Ettus [Ett09] hergestellte Universal Software Radio Peripheral (USRP) erlaubt es, die gesamte Signalverarbeitung mittels Software zu realisieren. Im Gegensatz zu einer für ein bestimmtes Einsatzgebiet konstruierten Spezialhardware können mit dem Software-defined Radio unterschiedliche Modulationsarten, Multiplex- und Medienzugriffsverfahren für den Frequenzbereich von 1 MHz bis zu 5,9 GHz umgesetzt werden. [Ett] Das gewährleistet eine größtmögliche Flexibilität, die es erlaubt, eine Reihe verschiedener Anwendungen wie RFID-Lesegeräte, WLAN-Empfänger, FM- Radiostationen oder GSM-Netzwerkkomponenten für das Radio Subsystem aufzubauen. Es existieren zwei Varianten am Markt, wobei das ältere USRP1 vom OpenBTS-Projekt unterstützt wird und das neue sich für Frequenzbandanalysen eignet.
Das Time Divison Multiplexing von GSM ist zeitkritisch. Ausführliche Experimente zeigten, dass der eingebaute Zeitgeber des USRP für einen langzeit-stabilen Betrieb nicht ausreicht. Deshalb wurde das USRP so modifiziert, dass sich verschiedene externe Zeitgeber anschließen lassen. Eine Variante besteht im Einsatz des Bausatzes FA-SY1, der von Funkamateuren genutzt wird. [7309] Der Taktgeber lässt sich über USB auf eine Frequenz zwischen 10 bis 160 MHz einstellen und weist anfänglich eine Abweichung von $\pm$ 20 ppm auf, welche durch eine Kalibrierung allerdings verringert werden kann. Für eine tempe-

raturunabhängige Frequenzstabilität besitzt der Taktgeber einen Heiztransistor, der über einen Temperaturfühler geregelt wird.
Da das USRP lediglich das High-Level-Sampling übernimmt, muss ein Linux-PC mit GNU Radio, die Signalverarbeitung der niedrigen Abtastraten übernehmen. Dabei stellt es lediglich eine allgemeine Schnittstelle zum USRP bereit, die aus Bibliotheken zur Signalverarbeitung und einem USB-Kernelmodul für die Ansteuerung der Hardware besteht. Erst mit Hilfe des OpenBTS Projekts wird daraus eine GSM-Basisstation. OpenBTS bildet hierzu das Mindestmaß einer GSM-Infrastruktur nach, wozu es bespielsweise über eine Art integrierte Mini-VLR verfügt, in dem die TMSI's verwaltet werden. Ebenfalls benötigt OpenBTS einen Asterisk-Server, um eine ganze Reihe von Aufgaben, wie die Identifikation und Authentifizierung (HLR) der Teilnehmer sowie das Führen von Telefongesprächen innerhalb von OpenBTS in das allgemeine Telefonnetz (TRAU) zu realisieren.
Gestartet werden kann OpenBTS mit dem Befehl `./OpenBTS`. Wichtig hierbei ist, dass die Konfigurationsdatei *OpenBTS.config* zuvor bearbeitet und entsprechende Parameter eingestellt wurden. Die wohl wichtigsten Konfigurationsparameter sind im „GSM" Abschnitt der Datei *OpenBTS.config* zu finden. Durch die Variable *GSM.Band 900* kann zwischen GSM 900 und 1800 gewechselt werden. Mittels *GSM.ARFCN 29* wird die entsprechende Frequenz eingestellt, ARFCAN 29 entspricht dabei 940.8 MHz. Durch die Variablen *GSM.MCC 922*, *GSM.LAC 667*, *GSM.CI 10* sowie *GSM.ShortName „OpenBTS"* wird eine GSM-Zelle mit dem Namen OpenBTS, dem Ländercode 922, dem Location Area Code 667 und der CellID 10 gestartet. Ältere Mobiltelefone zeigen als Netzname in der Netzliste „922 55" oder „Nor 55" an. Die 55 entspricht dem festgelegten Mobile Network Code (*GSM.MNC 55*). Diese Einstellungen lassen sich verwenden, um „Original"-Zellen zu simulieren.

3 GSM-Monitoring mit Wireshark und USRP oder Mobiltelefon

Wie für das Verständnis von TCP/IP auch, ist es hilfreich die verschiedenen Netzwerkprotokolle auf unterschiedlichen Layern der Protokoll-Stacks analysieren zu können. Das fängt auf der physikalischen Schicht mit der Ermittlung von Funkzellen an und setzt sich durch höhere Schichten und die Interpretation der Kanäle bis hin zu den Rahmenstrukturen fort. Auf diese Weise lässt sich beispielsweise die Frequenzverteilung in einem bestimmten Gebiet sichtbarmachen, zeigen wie das Einbuchen eines Mobiltelefons ins GSM-Netz erfolgt oder wie während geführter Telefonate die Qualität der Verbindung überwacht und bei Bedarf ein Handover eingeleitet wird. Diese Untersuchungen lassen sich sowohl im echten Mobilfunknetz als auch mit der selbstgebauten Basisstation vornehmen.

Nokia Netzmonitor Einige ältere Nokia-Mobiltelefone verfügen über einen Netzwerkmonitor, der über das gängige Menü normalerweise nicht zugänglich ist und erst mittels spezieller Software freigeschaltet werden muss.[1] Mittels dieses Monitors lassen sich Parameter wie Kanalzuteilung (CH), Leistungsregelung, Cell-ID (CID), Informationen über

[1] Die Vorgehensweise unterscheidet sich von Gerät zu Gerät. Eine ausführliche Anleitung für verschiedene Nokia Modelle findet sich auf der Homepage nokiaport.de.

Nachbarzellen (Display 03; erste Spalte ist der Kanal, dritte Spalte die Empfangsstärke) und Handover ermitteln. Vier dieser Netzmonitor-Displays eines Nokia 3310 sind in Abbildung 2 dargestellt.

Abbildung 2: Der Netzmonitor im Menü eines Nokia 3310 mit Informationen zu den einzelnen empfangenen Basisstationen.

USRP und GNU Radio-Spektrumsanalyse GNU Radio enhält eine Vielzahl an Beispielprogrammen, wie ein Softwareoszilloskop oder einen Spektrumsanalysator. Letzteres ist ein Python-Skript (*usrp_fft.py*), das sich für Untersuchungen und Experimente der GSM-Frequenzbänder nutzen lässt. Mit Hilfe dieses Analysators lassen sich Base Transciever Stations aufspüren. Mit folgendem Befehl kann ein Scanvorgang begonnen werden: `usrp_fft.py -R A -d 8 -g 47 -f 928M`. Dieser Befehl sorgt dafür, dass um die Frequenz von 928 MHz ($\pm$ 4 MHz) nach BTS gescannt wird. Das Ergebnis und die Einstellungen, wie Average, können der Abbildung 3 entnommen werden.

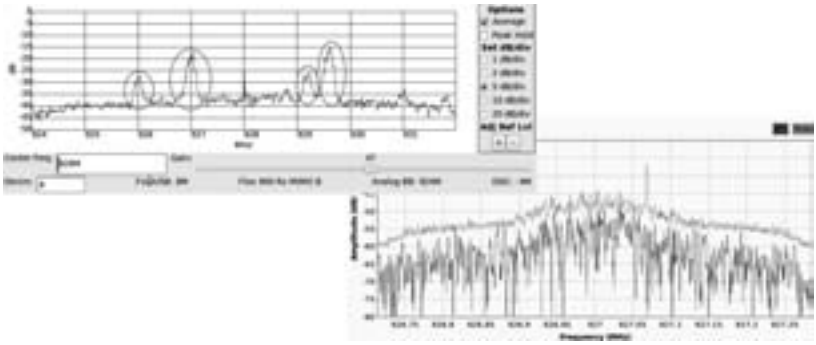


Abbildung 3: Spektrumsanalyse im Bereich von 924 - 932 MHz (oben) bzw. genauere Betrachtung (unten) eines BTS-Kanals bei 927 MHz (Decim=112) mittels GNU Radio-Skript: *usrp_fft.py*

Es ist deutlich zu erkennen, dass es mehrere Ausschläge im Bereich um 928 MHz gibt (rot markiert). Hierbei handelt es sich um 200 kHz breite Kanäle. Für eine genauere Betrachtung wurde mit einer feineren Auflösung der Frequenz (=Decim) der größte Ausschlag (BTS mit bester Sende- bzw. Empfangsstärke) bei 927.0 MHz gewählt. Dies erfolgt mit dem Befehl: `usrp_fft.py -R A -d 112 -g 32 -f 927M`. Außerdem wurde in Abbildung 3 die Option Peek Hold verwendet. Diese sorgt dafür, dass der größte Ausschlag gespeichert wird (grüne Linie). Genau +67,7 kHz von der Kanalmitte entfernt ist deutlich ein Ausschlag (Peek) zu erkennen. Hierbei handelt es sich um ein FCCH-Paket,

das periodisch alle zehn Pakete im Zeitschlitz 0 übertragen wird. Es dient der Frequenzkorrektur und zur Auswahl der Zelle des BTS mit der besten Empfangsfrequenz.

AirProbe und GSSM mit USRP Bei der Softwaresammlung AirProbe handelt es sich um ein GSM-Sniffer-Projekt des Chaos Computer Clubs. [Clu09] Ziel dieses Projekts ist es, ein Analyse-Tool zu schaffen, das in der Lage ist, GSM-Daten auf dem Air-Interface zu analysieren. Der dritte und vielleicht wichtigste Aspekt des Projekts ist es, die Sicherheitslücken des GSM-Standards zu demonstrieren. AirProbe gliedert sich in drei Hauptteile: Erfassung von Daten, Demodulation und Analyse.
Für sämtliche Tests kam die Mitte 2009 aktuelle AirProbe-Version aus dem Git-Repository des Chaos Computer Clubs zum Einsatz, die durch einen weiterentwickelten GSM-Receiver gepatcht wurde.[2] Der Ordner *gsmdecode/src/python* des AirProbe Verzeichnisses enthält zwei Skripte: *capture.sh* und *go.sh*. Ersteres dient dazu, mittels USRP und GNU Radio Daten aufzuzeichnen, das zweite, diese zu dekodieren. Vorher ist eine aktive Frequenz zu ermitteln, auf der eine Funkzelle sendet. So liess sich durch mehrere Tests auf verschiedenen Frequenzen mittels *go.sh* eine E-Plus Funkzelle auf 927.0 MHz identifizieren. Diverse Parameter wie Mobile Country und Network Code, Ordinary Subscribers sowie Emergency Call ließen sich darüber hinaus sichtbar machen.

GSSM Das Softwarepaket GSSM kann GSM Base Station Control Channels überwachen. Die Analyse der gesammelten Pakete erfolgt in einem gepatchten Wireshark mittels eines virtuellen TUN-Interfaces. GNU Radio übernimmt dabei die Demodulation und Dekodierung der einzelnen GSM-Pakete. Folgende Kontrollkanäle (zwischen BTS und MS) können mittels GSSM v.0.1.1.1a decodiert werden: FCCH, SCH, BCCH, PCH (nur Downlink), AGCH (nur Downlink), SACCH, SDCCH
Um die live mitgeschnittenen Daten sichtbar zu machen, muss Wireshark gestartet und das erstellte GSM-Interface zur Überwachung ausgewählt werden. Einen Ausschnitt der ermittelten GSM-Pakete in Wireshark wird in Abbildung 4 dargestellt.
Bisher ist GSSM lediglich in der Lage, GSM-Pakete von der BTS zur MS zu überwachen, aber nicht umgekehrt. Die Um-Schnittstelle wurde nur teilweise implementiert und viele Pakete kann Wireshark nicht korrekt interpretieren, da sie über eine abweichende Protokoll-Beschreibung verfügen. Die Identifizierung kann beispielsweise durch einen unterschiedlichen Frame-Type fehlschlagen.

GSM Dekodierung durch Nokia 3310 und Wireshark Das Mobiltelefon Nokia 3310 ist in der Lage, GSM-Nachrichten aus einem Gammu Trace Log zu dekodieren. Es ist möglich, Signalisierungsprozesse auf Layer 2 (LAPDm) in Sende- und Empfangsrichtung sichtbar zu machen. Diese Tatsache beruht darauf, dass die Entwickler eine Loggingfunktion eingebaut hatten. Die generierten XML-Dateien können mit Wireshark geöffnet und analysiert werden. Alternativ kann zur Analyse der aufgezeichneten Dateien auch das Programm *Gsmdecode* des Chaos Computer Clubs verwendet werden. Es ist genau wie Wire-

[2] Genauere Informationen auf der Webseite: AirProbe Git-Repository, `git://svn.berlin.ccc.de/`. Patch von Piot Krysik unter `http://home.elka.pw.edu.pl/_pkrysik/GSM`.

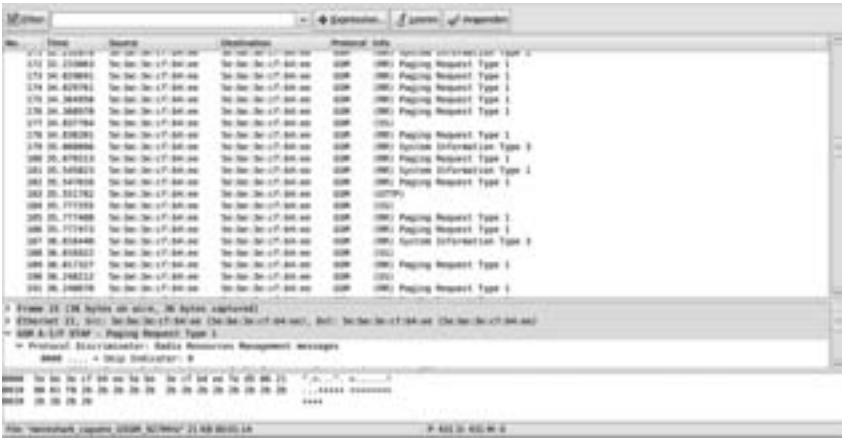


Abbildung 4: Ausschnitt eines GSM-Paketes in Wireshark

shark in der Lage, GSM-Nachrichten zu dekodieren.[3] Hardwareseitig wird ein Nokia 3310 Mobiltelefon und ein spezielles MBUS NK-33 Datenkabel benötigt.[4] Eine genaue Installationsanleitung für die Software kann dem AirProbe Wiki des CCC entnommen werden.[5] Es werden die Pakete *gammu*,[6] *Wireshark* (Version 1.2.1) und *dialog* benötigt.

Abbildung 5 zeigt einen Gesprächsaufbau des Nokia 3310 über das T-Mobile Netz im Wireshark. Die entsprechenden Pakete ließen sich parallel mittels Gammu-Software aufzeichnen und das Log-File danach mit Wireshark betrachten. Darüber hinaus wurde eine SMS-Nachricht mittels Nokia E71 an das Nokia 3310 gesendet und mittels Gammu-Tracelog mitgeschnitten. Der Nachrichteninhalt der SMS konnte auf Grund der eingeschalteten Verschlüsselung nicht eingesehen werden. Bei einem Gesprächsaufbau eines iPhone 2Gs zu einem Nokia 3310 über OpenBTS wird im Vergleich deutlich, dass in OpenBTS keine Verschlüsselung verwendet wird. Dasselbe gilt für SMS. Dazu wurde mittels der OpenBTS Konsole an das Nokia 3310 eine SMS-Nachricht geschickt, um die dabei ablaufenden Signalisierungsprozesse aufzuzeichnen. Der Inhalt dieser Nachricht „Das ist ein Test“ konnte in Wireshark unverschlüsselt mitgelesen werden.

4 Der IMSI-Catcher aus dem Elektronikmarkt

Der erste IMSI-Catcher mit dem Namen GA090 wurde von der deutschen Firma Rohde & Schwarz 1996 in München vorgestellt. Er wurde ursprünglich als Test- und Messsystem

[3] `https://svn.berlin.ccc.de/projects/airprobe/attachment/wiki/tracelog/gsmdecode-0.7bis.tar.gz`

[4] N-33 Nokia Cable 3310, 3330, 3390 with MBUS Interface (compatible), `http://ucables.com/ref/NK-33`

[5] Tracelog - AirProbe, `https://svn.berlin.ccc.de/projects/airprobe/wiki/tracelog`

[6] `http://www.gammu.org/wiki/index.php?title=Download` - Version: 1.26.1

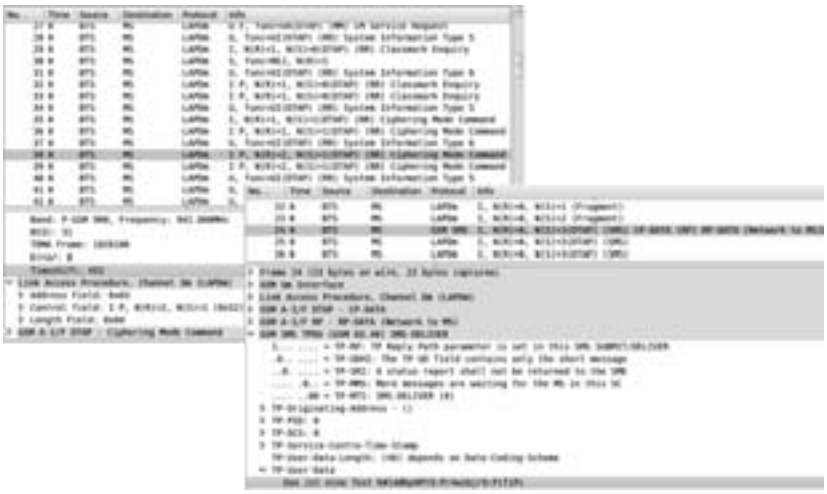


Abbildung 5: Wireshark-Mitschnitt: Gesprächsaufbau mit Verschlüsselungskommando im T-Mobile Netz (oben) und Empfang einer SMS von OpenBTS an Nokia 3310 (unten)

konstruiert und später zur Bestimmung der Endgerätekennung von Mobile Stations weiterentwickelt. [Han]
Auf Basis der USRP-Hardware und OpenBTS konnte ein eigener IMSI-Catcher entwickelt werden, der sowohl die IMSI als auch die IMEI auslesen, sowie alle aktuellen Gespräche mit Zielrufnummer anzeigen und aufzeichnen kann. [Weh09] Die Funktionsweise des Open Source IMSI-Catchers (Abbildung 6) unterscheidet sich vom Standard-IMSI-Catcher dahingehend, dass für die Weiterleitung der Daten keine an den IMSI-Catcher angeschlossene MS verwendet werden kann. Diese Beschränkung ergibt sich auf Grund der verwendeten Hard- und Softwarekomponenten. Daher ist der Aufbau des IMSI-Catchers und die Authentifizierung gegenüber dem Standard IMSI-Catcher leicht verändert. Der unverschlüsselte Datenverkehr wird nicht mehr über eine MS, sondern über den Computer und darin installiertem Asterisk-Server weitergeleitet. Dieser Server ermöglicht es, Festnetz- und Mobilfunkgespräche zu führen. Wie beim Standard IMSI-Catcher wird jedoch nicht die Identität des Teilnehmers vorgetäsucht. Aus diesem Grund muss die Rufnummerübermittlung deaktiviert werden. Der angerufene Teilnehmer bekommt somit einen Anruf von einem „unbekannten Teilnehmer“. Damit die MS die vom IMSI-Catcher simulierte Zelle, nicht von einem realen Netz unterscheiden kann, muss der IMSI-Catcher ein entsprechendes Netz des gewünschten Anbieters vortäuschen. Hierfür werden diverse Konfigurationseinstellungen in der *OpenBTS.conf* vorgenommen. Wichtig für das Simulieren sind lediglich der richtige Country Code (*MCC*), der vorzutäuschende Netzanbieter Code (*MNC*), die Frequenz sowie der Name der Funkzelle (*Shortname*), der identisch dem Netzanbieter sein muss. Allerdings darf die Frequenz nicht die selbe sein. Die notwendigen Informationen über aktuelle Basisstationen beschafft man mit Hilfe der bereits gezeigten Frequenzanalyse. Alle anderen Parameter sind irrelevant, da diese Informationen der MS lediglich dazu dienen, ihren Standort (LAC und CID) zu bestimmen.

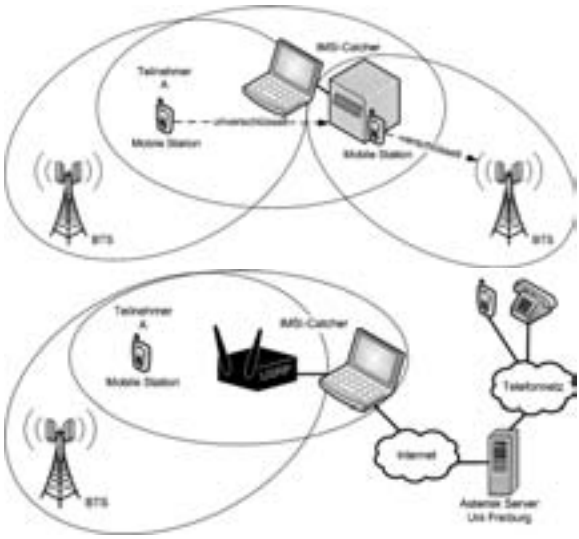


Abbildung 6: Funktionsweise eines Standard IMSI-Catcher (oben) und Open Source IMSI-Catcher mit USRP und Asterisk-Server (unten)

Insgesamt existieren drei Möglichkeiten, wie sich eine MS in ein vorgetäuschtes Netz des IMSI-Catchers einbuchen kann. Wie sich durch diverse Versuche herausgestellt hat, ist es dabei unerheblich, ob der Teilnehmer eine manuelle oder automatische Netzauswahl eingestellt hat. Da die MS das Netz des IMSI-Catchers nicht von einem Originalnetz unterscheiden kann, ist dieses Verhalten leicht zu erklären.

1. Fall - Zielnetz nicht vorhanden
   Die MS besitzt keine Konnektivität und befindet sich im Suchmodus (Normal Cell Selection), wodurch nacheinander verschiedene Frequenzen nach einer aktiven BTS gescannt werden. In diesem Fall muss der IMSI-Catcher lediglich eine beliebige Frequenz, den Ländercode 262 als auch den benötigten Netzanbietercode und Shortname einstellen. Sobald die MS diese Frequenz scannt, versucht sie sich einzubuchen.

2. Fall - Zielnetz vorhanden
   Schwieriger ist der Fall eines vorhandenen aktiven Netzes, in dem die MS eingebucht ist. Hier existieren zwei Möglichkeiten, eine MS dazu zu bringen, sich beim IMSI-Catcher anzumelden. Eine Variante besteht darin, einen manuellen Zellwechsel anzustoßen. Eine weitere Variante, die Frequenz zu stören, auf der die MS im Netz des Anbieters eingebucht ist, damit die MS sich in den IMSI-Catcher einbucht.

   (a) **Erzwungener Zellwechsel:** Die Grundidee bei diesem Szenario ist, auf Grund der Nachbarschaftsliste einen Zellwechsel der MS in den IMSI-Catcher zu erzwingen.

(b) **Jammer:** Ein GSM-Jammer ist ein Störsender mit dem Ziel, die Frequenz, in der die MS eingebucht ist, zu verrauschen. Mit Hilfe des Jammers verliert die MS die Verbindung zur aktuellen BTS. Sie wechselt in den Frequenzsuchmodus mit dem Ziel, dass der IMSI-Catcher anschließend als Netz ausgewählt wird.

Gegenwärtig bietet GSM keinen ausreichenden Schutz vor einem IMSI-Catcher. Die minimale Schutzfunktion, unverschlüsselte Verbindungen anzuzeigen, wird typischerweise durch die Provider auf der SIM abgeschaltet. Selbst das aktuellere UMTS bietet nicht den notwendigen Schutz, da mit einem Jammer die Frequenzen von Basisstationen gestört werden können. Dem Mobiltelefon wird mit Hilfe einer „fallback"-Funktion die Nutzung des GSM-Netzes ermöglicht, falls kein UMTS-Netz verfügbar ist. Somit muss das Mobiltelefon lediglich dazu gebracht werden GSM zu nutzen. Wird allerdings ausschließlich das UMTS-Netz verwendet, muss ein anderer IMSI-Catcher entwickelt werden, der sich an dem Standard IMSI-Catcher orientiert und Daten an das Originalnetz weiterleitet. Die Funktionsweise eines UMTS-IMSI-Catchers (Abbildung 7) ist relativ ähnlich und läuft in drei Phasen ab: [MW04]

1. Die IMSI bzw. TMSI der Mobile Station muss beim initialen Registrierungsprozess gespeichert werden.

2. Der IMSI-Catcher überträgt die gespeicherte IMSI zum Originalnetz und bekommt die Zufallszahl RAND und das Authentication Token (AUTN) als Antwort. Der IMSI-Catcher trennt dann die Verbindung und speichert RAND und AUTN.

3. Der IMSI-Catcher überträgt anschließend die RAND und das AUTN an die Mobile Station, die die Korrektheit von AUTN anerkennt, da das Token aktuell ist. Die Mobile Station bucht sich anschließend in den IMSI-Catcher ein, der wiederum die Verschlüsselung ausschaltet.

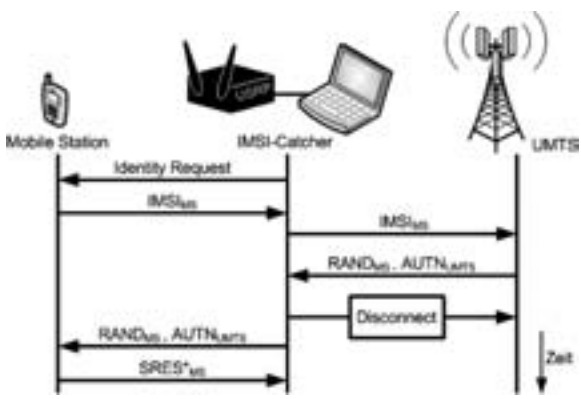


Abbildung 7: Funktionsweise eines UMTS-IMSI-Catchers

5 Fazit

Der Sicherheitsstandard von GSM lässt sich mit dem des Internets von vor 15 Jahren vergleichen. Insofern ist sicherlich in der nächsten Zeit mit weiteren Angriffen zu rechnen, beispielsweise mit einer Denial-of-Server, die auf dem 26C3 gezeigt wurde ([Spa09], [PN09]). Zunehmender SMS-SPAM oder der Versuch der Config-over-the-Air könnten weitere Problemvektoren darstellen: Gelingt es, verschiedene Teilnehmer in ein durch OpenBTS simuliertes Netz zu locken, können diese mit beliebig vielen SMS-Nachrichten überflutet werden. Anders als beim weit verbreiteten E-Mail Spam, der vorhandene Empfängeradressen voraussetzt, benötigt man keine gültigen Mobilfunknummern. Die MS müssen sich lediglich im Sende- bzw. Empfangsradius einer OpenBTS-Zelle befinden und sich einbuchen. Weitaus gefährlicher könnte es werden, Mobiltelefone per SMS zu manipulieren. Hierzu könnte beispielsweise der Austausch des WAP-Gateways, Internet oder SMS-Gateways oder auch die Manipulation der Mobiltelefon Firmware gehören.
Ein wesentlicher Nachteil gegenüber den Untersuchungen der Internet-Protokolle bleibt bestehen: GSM lässt sich nur mit einer Testlizenz bei Tageslicht benutzen. Andernfalls bleibt nur der abgeschirmte Tiefkeller.

Literatur

[7309] Box 73. *Box 73 Amateurfunkservice GmbH*. WWW-Dokument, `http://www.box73.de/catalog/`, 09 2009.

[Clu09] Chaos Computer Club. *airprobe*. WWW-Dokument, `https://svn.berlin.ccc.de/projects/airprobe/`, 09 2009.

[Ett] Ettus. *Brochure for the entire USRP product family*. PDF-Dokument, `http://www.ettus.com/downloads/er_broch_trifold_v5b.pdf`.

[Ett09] Ettus. *Ettus Research LLC*. WWW-Dokument, `http://www.ettus.com/`, 10 2009.

[Han] Uni Hannover. *IMSI-Catcher - Wanzen fuer Handys*. WWW-Dokument, `http://www.iwi.uni-hannover.de/lv/ucc_ws04_05/riemer/literatur/imsi-catcher.htm`.

[MW04] Ulrike Meyer and Susanne Wetzel. A man-in-the-middle attack on UMTS. In *WiSe '04: Proceedings of the 3rd ACM workshop on Wireless security*, pages 90–97, New York, NY, USA, 2004. ACM.

[PN09] Chris Paget and Karsten Nohl. *GSM: SRSLY?* WWW-Dokument, `http://events.ccc.de/congress/2009/Fahrplan/attachments/1519_26C3.Karsten.Nohl.GSM.pdf`, 12 2009.

[Spa09] Dieter Spaar. *Playing with the GSM RF Interface*. PDF-Dokument, `http://events.ccc.de/congress/2009/Fahrplan/attachments/1507_Playing_with_the_GSM_RF_Interface.pdf`, 2009.

[Weh09] Dennis Wehrle. *Open Source IMSI-Catcher*. PDF-Dokument, `http://www.ks.uni-freiburg.de/php_arbeitdet.php?id=166`, 10 2009.

Netzgüte

Schwachstellensuche - Qualitätsüberwachung im Netz durch Klassifizierung des HADES One-Way Delays

Dr. Stephan Kraft, Birgit König, Martin Gründl
WiN-Labor
Universität Erlangen-Nürnberg
Martensstr. 1, 91058 Erlangen
[stephan.kraft, birgit.koenig,martin.gruendl]@dfn.de

Abstract: HADES ist ein im WiN-Labor an der Universität Erlangen entwickeltes System zur Ermittlung qualitätsrelevanter Daten wie IP-Paketlaufzeit und Paketverluste in Computernetzwerken. Gemessene und statistisch bewertete Paketlaufzeiten lassen Rückschlüsse zu, wie die Qualität von Netzwerkverbindungen einzuordnen ist und wo kritische Netzwerksituationen auftreten bzw. auftreten können. In dieser Arbeit wird das generelle Verfahren der Datengewinnung, deren statistische Analyse und die Ergebnisse in Form eines Rankings auf Layer3-Ebene vorgestellt.

1 Einleitung

Um die Dienstgüte von Netzwerkverbindungen überwachen und bestimmen zu können, hat das WiN-Labor der Universität Erlangen im Rahmen von Projekten des DFN-Verein [DFN09] im X-WiN [XWI] und im europäischen Netzwerk GÉANT [GEA] ein Messsystem [HAD09] entwickelt, welches qualitätsrelevante Daten wie One-Way Delay (Paketlaufzeit), One-Way Delay Variation (Jitter) und Paket Loss (Paketverluste) ensprechend [PAMM98, ALM99a, ALM99b, DC02] ermittelt.
Dazu werden von einer Sendestation Gruppen von UDP-Paketen in konfigurierbaren Abständen erzeugt. Die Pakete werden mit einer Sequenznummer und einem aktuellen Zeitstempel versehen und an eine Empfangsstation, die die aktuelle Empfangszeit bestimmt, gesendet. Daraus werden One-Way Delay, Delay Variation und Paketverluste der gemessenen Verbindungen ermittelt.
Eine mathematisch-statistische Analyse [HOL08] wertet die Daten durch vergleichendes Klassifizieren aus und hilft damit, Schwachstellen im Netzwerk zu finden.

2 Hades-Messsystem

2.1 IP Performance Metrics

Die Idee des Messverfahrens basiert auf Ansätzen der IETF. In der Working Group IP Performance Metrics (IPPM) wurde dazu 1998 ein umfangreiches Rahmenwerk

verabschiedet, welches Definitionen zur Messung der Netzperformance beinhaltet [PAMM98]. Damit sollen Messverfahren und deren Auswertung standardisiert werden. Zu den wichtigsten definierten Metriken gehören One-Way Delay (OWD – Laufzeitverzögerung), IP Delay Variation (IPDV, OWDV – Jitter, Differenz der OWDs aufeinanderfolgender Pakete) und Packet Loss (Anteil der verlorenen Pakete in einem bestimmten Zeitraum), anhand derer man die Dienstgüte bestimmen kann [ALM99a, ALM99b].

2.2 Zeitsynchronisation

Die Qualität der gemessenen Metriken hängt entscheidend von der Genauigkeit des Zeitstempels ab.
Das *Network Time Protocol* (NTP) ist eine Möglichkeit zur Uhrensynchronisation in paketvermittelten Kommunikationssystemen. Einem NTP-Prozess ntpd wird in regelmäßigen Abständen durch externe Signale von GPS-Satelliten oder NTP-Servern die aktuelle Uhrzeit übermittelt. Die Zeitsynchronisation wird durch die Einstellung der Frequenz der lokalen Uhr erreicht. Die aktuelle Version erreicht im Internet eine Genauigkeit im Bereich von 10 Millisekunden [NTP1, NTP2].
Beim *Global Position System* (GPS) handelt es sich um ein satellitengestütztes System zur weltweiten Positionsbestimmung, ursprünglich für den militärischen Gebrauch konzipiert. Von jedem Punkt der Erde sind vier Satelliten erreichbar. Während einer der Satelliten die Quarzuhr des GPS-Empfängers synchronisiert, dienen die anderen drei zur Positionsbestimmung [FAA]. Man kann sich der hohen Zeitgenauigkeit bedienen und die Zeitsynchronisation von unter 250 Nanosekunden nutzen.
Da die One-Way Delay Werte im Bereich von 10 Millisekunden liegen, ist NTP über das Netz nicht genau genug. Somit ist die gewählte Alternative eine GPS-Karte, die über eine angeschlossene GPS-Antenne die Signale der Satelliten empfängt und die Systemuhr via NTP synchronisiert [HOL08]. Die Genauigkeit der NTP-Synchronizität mittels GPS liegt bei 10 Mikrosekunden.

2.3 Messverfahren

Gemessen wird auf Messstationen, die aktiv UDP-Testpakete generieren, diese ins Netz einschleusen und Pakete von anderen Messrechnern empfangen [HKK06].
Der Quellrechner versieht die Pakete vor dem Senden mit einem präzisen Zeitstempel. Die zu versendenden Pakete werden gruppiert und in kurzen zeitlichen Abständen verschickt. Startzeitpunkt, Anzahl der Pakete, Paketgröße, zeitlicher Abstand der Pakete zueinander und das Ziel sind dabei variabel einstellbare Parameter.
Der Zielrechner wiederum empfängt die Pakete und speichert die Eingangszeit. Die Daten werden vom Zielrechner abgeholt und dann in einem weiteren Verfahren zur Bestimmung der Dienstgüte genutzt.
Derzeit wird alle 30 Sekunden eine Gruppe von neun Paketen mit 42 Bytes Größe verschickt. Die einzelnen Pakete haben einen Abstand von fünf Millisekunden zueinander, um Kollisionen zu vermeiden.

2.4 Verbreitung

Ausgehend von der ersten Messstation im deutschen Forschungsnetz X-WiN, installiert im Sommer 2002, hat sich das Messsystem über das Europäische Forschungsnetz GN (GÉANT) hinaus weltweit verbreitet.
Tabelle 1 gibt einen Überblick über die Beteiligung an verschiedenen Projekten, die Anzahl der mit Messstationen versehenen Standorte und die ungefähre Anzahl von Messstrecken.

Tabelle 1: Überblick über den derzeitigen Ausbaustand der HADES Messysteme.

Projekt	*Anzahl der Standorte*	*Anzahl der Messstrecken*
X-WiN	**57**	**Ca. 3500**
GÉANT	**36**	**Ca. 1200**
MDM[1]	**23**	**Ca. 500**
LHCOPN[2]	**10**	**Ca. 40**

3 Performance-Klassifizierung

Nachdem die Performance-Messungen zuverlässig verwertbare Daten liefern, besteht eine nächste Aufgabe darin, die ermittelten Daten zu analysieren, um Aussagen über die Übertragungsqualität in Netzwerken zu bekommen.
In einer vom WiN-Labor betreuten Diplomarbeit [HOL08] wurden mehrere statistische Modelle beschrieben, die beobachtete OWD (One-Way Delay) Messdaten durch wenige Parameter charakterisieren. Dazu werden 15-Minuten Intervalle in Qualitätsklassen eingruppiert und mit einer Gewichtung aufsummiert. Mittels Klassifizierung der OWD – Muster wird ein Analysesystem entwickelt, das die aktuelle Qualität von Netzwerkverbindungen automatisch einordnen und kritische Netzwerksituationen erkennen kann.

3.1 Routing Delay und Performanceklassen

Der *routing delay* ist im Gegensatz zum *intrinsic delay* der variable Teil des OWD. Während der *intrinsic delay* die minimale Zeit beschreibt, die das Signal braucht, um die aktiven und passiven Komponenten des IP-Pfades zu durchlaufen, wird der *routing delay* durch das variable Verhalten der Komponenten auf der Strecke bestimmt. Der *routing delay* wird durch Subtraktion des *intrinsic delays* vom OWD bestimmt.

Der *routing delay* (Viertelstundenwert) lässt sich folgendermaßen klassifizieren:

[1] perfSONAR Multi-Domain Monitoring, domänüberspannendes Monitoring
[2] s. Kapitel 4

- **excellent:** Diese Klasse beschreibt den bestmöglichen Zustand einer Strecke mit einem stabilen *routing delay*.
- **fair:** Damit wird eine leichte Verschlechterung einer Strecke durch eine wachsende Varianz des *routing delay* charakterisiert. Es gibt einzelne statistische Ausreißer.
- **poor:** Man sieht eine größere Streuung der Messwerte, was auf eine leichte Überlast einer Strecke hinweisen kann.
- **bad:** Diese Klasse kennzeichnet den schlechtesten Zustand einer Strecke. Es gibt eine große Streuung der Messwerte, möglicherweise durch Überlast.

3.2 Ranking

Ein auf Grundlage der Diplomarbeit entwickeltes Analysetool bestimmt die durchschnittliche Performance beobachteter Verbindungen über einen längeren Zeitraum (ein oder mehrere Tage). Im *Ranking* werden die Verbindungen miteinander verglichen. Dazu wird die Klasse *excellent* mit dem Faktor 4 gewichtet, die Klasse *fair* mit 3, die Klasse *poor* mit 2 und die Klasse *bad* mit 1. Das Vorkommen der Viertelstundenwerte je Klasse wird gezählt und auf einen Tag aggregiert. Durch die Gewichtung der einzelnen Klassen ergibt sich ein Score, der den Rang bestimmt. Der maximal erreichbare und somit „beste“ Wert für eine Verbindung und einen Tag beträgt daher 384, während im „schlechtesten“ Fall ein Score von 96 zu Buche steht.
Der dem Ranking zugrundeliegende OWD gibt keine Auskunft über die Gründe für eine bestimmte Performance auf den Verbindungen. So ist es beispielsweise durchaus verständlich, wenn das OWD bei „langen“ Strecken oder abhängig vom zurückgelegten Weg (Anzahl der Hops) größer ist. Auch eine Überlast kann zu Phänomenen im OWD führen.

4 Ranking am Beispiel des LHCOPN

4.1 Das LHCOPN

Durch den Betrieb des Large Hadron Collider (LHC) am CERN fallen große Mengen Daten an, die an verschiedenen Einrichtungen überall auf der Welt gespeichert und verarbeitet werden sollen. Das LHCOPN (Large Hadron Collider Optical Private Network) ist das Netzwerk, welches Tier0- (Datenquelle) und Tier1- (erste Verarbeitung und Speicherung) Standorte miteinander verbindet. Daran schließen sich Tier2-Standorte an, in der Regel Universitäten und andere wissenschaftliche Einrichtungen.

4.2 Laufzeitmessungen im LHCOPN

Das WiN-Labor beteiligt sich an diesem Projekt durch eine aktive Überwachung der Performance des zugehörigen Routernetzes.

An allen Tier0/Tier1-Standorten wurden HADES-Messboxen installiert: SARA/NL (Amsterdam, **NL-T1**), DE-KIT (Karlsruhe, **DE-KIT**), PIC (Barcelona, **ES-PIC**), IN2P3 (Lyon, **FR-CCIN2P3**), CERN (Genf, **CH-CERN**), CNAF (Bologna, **IT-INFN-CNAF**), NDGF (Kopenhagen, **NDGF**), BNL (New York, **US-T1-BNL**), ASGC (Taipeh, **TW-ASGC**), TRIUMF (Vancouver, **CA-TRIUMF**), FNAL (Chicago, **US-FNAL-CMS**), RAL (Rutherford, **UK-T1-RAL**).

Eine Darstellung des gemessenen OWDs zeigt Abbildung 1.

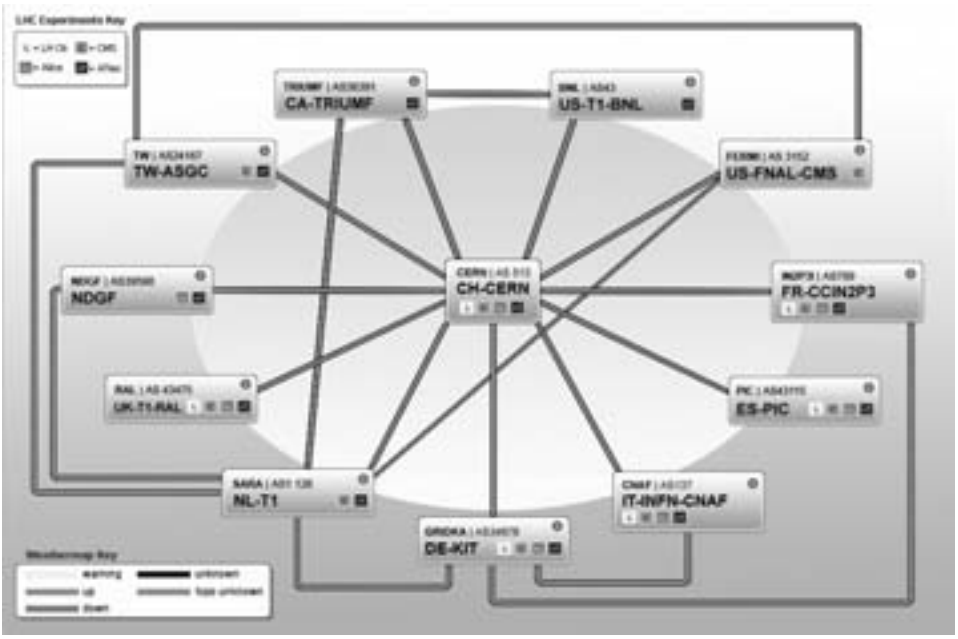


Abbildung 1: Topologie und HADES-Messungen im LHCOPN.

4.3 Ranking

Im LHCOPN werden momentan 40 Messstrecken (20 Verbindungen, jeweils Hin- und Rückrichtung) betrachtet und bewertet.
Für die folgenden Beispiele wurden über einen Zeitraum von 10 Tagen die jeweils 10 schlechtesten Verbindungen pro Tag statistisch analysiert.

Verlauf

Die Tabelle 2 zeigt exemplarisch zwei Strecken, die in der Statistik erfasst werden, aber einen unterschiedlichen Verlauf im entsprechenden Zeitraum aufweisen.

Während die Verbindung von TW-ASGC-HADES nach CH-CERN-HADES an jedem der 10 Tage mit wechselndem Rank unter den 10 schlechtesten Leitungen ist (Anzahl), an vier Tagen sogar als schlechteste Leitung (Rang 1), findet man die Verbindung von IT-INFN-CNAF-HADES nach CH-CERN-HADES nur an zwei Tagen. Das zeigt sich auch im unterschiedlichen, über die 10 Tage gemittelten Score. Je niedriger der Score, desto schlechter ist die Qualität.

Tabelle 2: Tagesranking zweier Beispielstrecken.

Messstrecke	Tag	1	2	3	4	5	6	7	8	9	10	Anzahl	Score
TW-ASGC -> CH-CERN	Rang	**4**	**3**	**1**	**7**	**7**	**1**	**1**	**1**	**1**	**1**	10	**199**
IT-INFN-CNAF -> CH-CERN	Rang	>10	>10	>10	>10	>10	**7**	>10	>10	>10	**9**	2	**257**

Gemittelte Scores

Abbildung 2 zeigt die gemittelte Summe des Scores über 10 Tage. Aufgrund der beschriebenen Gewichtung nimmt die Qualität der Verbindungen von oben nach unten ab.

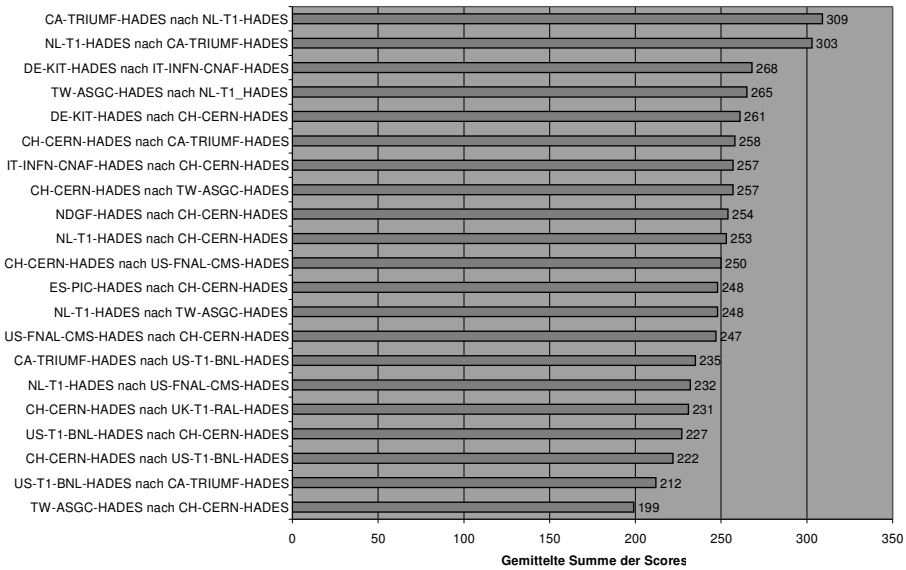


Abbildung 2: Gemittelte Summe der Scores im LHCOPN über 10 Tage.

Von den 40 im LHCOPN überwachten Verbindungen werden 21 in der Statistik aufgeführt. D.h. von den 21 Strecken ist jede mindestens einmal unter den schlechtesten 10 Strecken eines Tages gewesen. Die zwei besten der 21 Strecken liegen mit einem gemittelten Score von 309 bzw. 303 (zum Vergleich: Maximalscore = 384) deutlich über der Qualität der schlechtesten Verbindung mit einem Score von 199. In Abbildung 5 sind OWD und OWDV dieser Verbindung zu sehen.

Vorkommen im Ranking

Zählt man die Häufigkeiten des Auftretens der Verbindungen im 10-Tages Intervall, erhält man eine Häufigkeitsverteilung, die ebenso als Indiz für die Qualität der Verbindung dienen kann. Die schlechtesten Strecken treten am häufigsten auf (Abbildung 3).

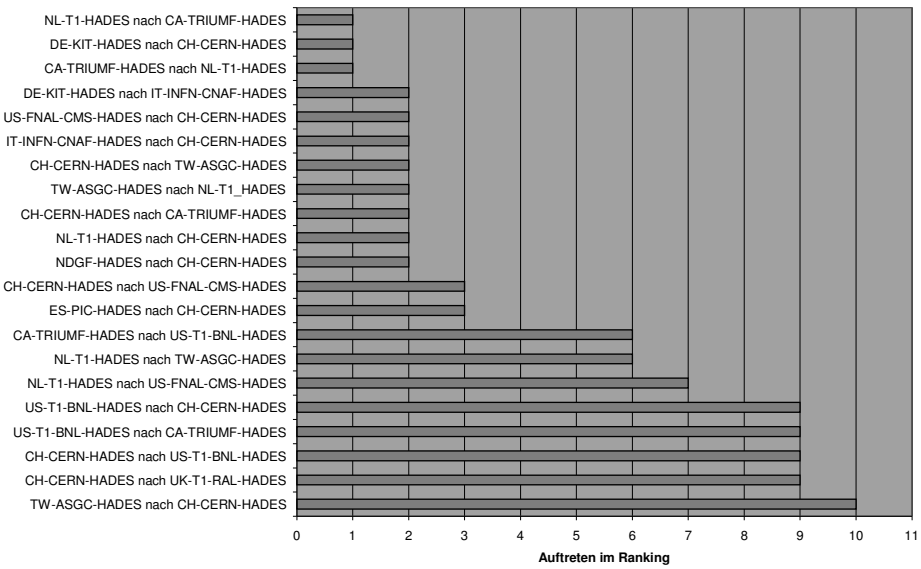


Abbildung 3: Aggregation des Auftretens im Ranking.

Die Strecke mit dem niedrigsten Score (s. Abbildung 6) ist auch hier mit dem häufigsten Auftreten im Ranking (10) am schlechtesten klassifiziert.

Aggregation nach Quelle und Senke

Eine Aggregation nach Quelle und Senke hilft bei der Suche nach Schwachstellen. Damit ist nicht nur ein Ranking der einzelnen Verbindungen möglich, sondern auch eine Bewertung der Standorte.
In Abbildung 4 wird das Auftreten eines Standortes (Senke) der letzten 10 Tage dargestellt. Zeigt sich eine relative Ausgeglichenheit beim Ranking der Standorte, liegen die Einbußen bei der Qualität der Verbindungen offensichtlich auf den Strecken selbst.

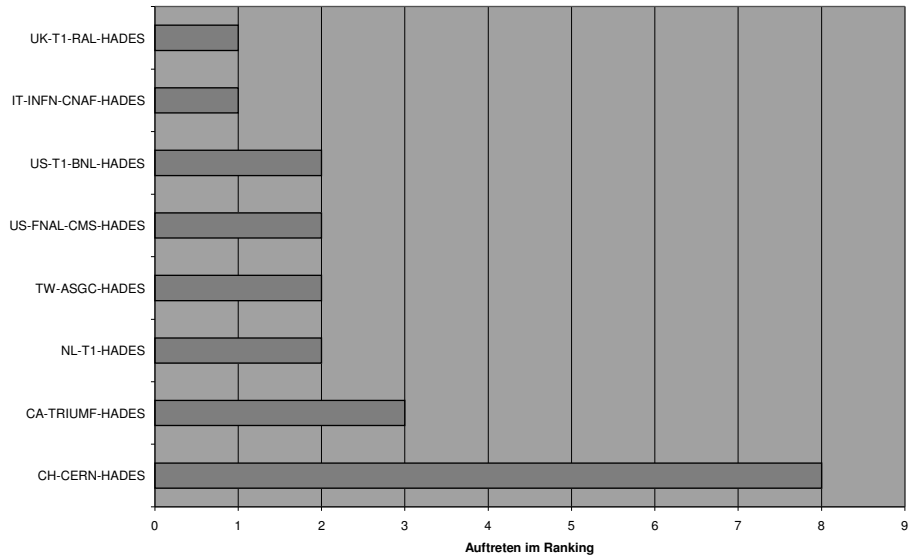


Abbildung 4: Auf Senken aggregiertes Auftreten im Ranking über 10 Tage.

In dem Fall sieht man, dass der Standort CERN wesentlich häufiger vorkommt als die anderen Standorte, was daran liegt, dass von den 40 gemessenen Verbindungen alleine 22 vom bzw. zum CERN gehen. Eine Quellen-Senken-Analyse ist sinnvoll für ein vollvermascht gemessenes Netz.

OWD und OWDV im 10-Tages-Verlauf (Abbildungen 5 und 6)

Betrachtet man den OWDV (One – Way Delay Variation, Jitter) der in Abbildung 2 an erster Stelle stehenden Verbindung (Abbildung 6) im Vergleich zur Verbindung an letzter Stelle (Abbildung 5), kann man die unterschiedliche Qualität der Verbindungen gut erkennen.
Während OWD und OWDV der Verbindung CA-TRIUMF-HADES nach NL-T1-HADES mit einem Score von 309 wenig Streuung aufweisen, ist bei gleicher Skalierung eine sehr breite Streuung auf der Verbindung TW-ASGC-HADES nach CH-CERN-HADES zu erkennen.
Ebenso kann man sehen, dass die Verbindung von CA-TRIUMF-HADES nach NL-T1-HADES wegen des ersten der ausgewählten 10 Tage im Ranking der schlechtesten 10 Verbindungen auftaucht. An diesem Tag war diese Strecke mit Rank 2 bewertet, also als zweitschlechteste Leitung. Da sie an den restlichen der 10 Tage nicht mehr unter den schlechtesten Verbindung war, ist der Score deutlich höher als bei einer über die gleiche Zeit dauerhaft schlechten Leitung.

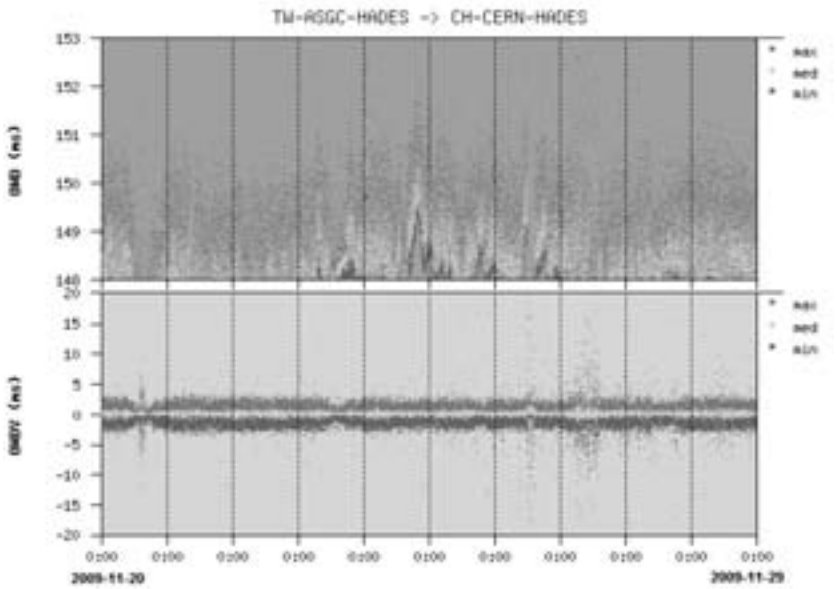


Abbildung 5: Zehn Tage Verlauf des OWD und OWDV einer Verbindung mit einem gemittelten Score von 199.

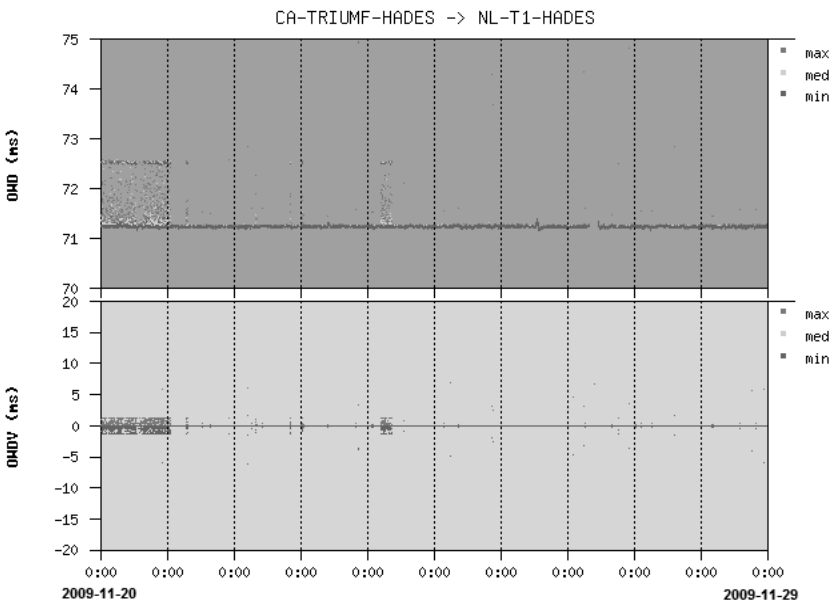


Abbildung 6: 10 Tage Verlauf des OWD und OWDV einer Verbindung mit einem gemittelten Score von 309.

5 Fazit

Die Analyse der mit dem HADES System am WiN-Labor des DFN am RegionalenRechenzentrum der Universität Erlangen-Nürnberg durchgeführten Laufzeitmessungen über einen längeren Zeitraum und damit die Bestimmung der Qualität gemessener Verbindungen ermöglicht eine Identifikation von „schlechten“ Verbindungen und liefert Informationen im Hinblick auf potentielle Schwachstellen im Netz. Das durchgeführte Ranking auf Tagesbasis und die nachfolgende Aggregation auf einen Zeitraum identifiziert sowohl Verbindungen mit kontinuierlich breiter Streuung der Messwerte, als auch Verbindungen, die temporär höhere Schwankungsbreiten aufweisen.
Für die Stellung von Verbindungen im Ranking kann es verschiedene Ursachen geben, beispielsweise die Anzahl der Hops, die Entfernung der Standorte, oder die Auslastung der Leitung (kontinuierlich, periodisch, singulär) selbst..
Die Bewertung durch das Ranking ermöglicht demnach zunächst eine Identifikation auffälliger Verbindungen, die Betrachtung der tatsächlichen Messverläufe kann dann zu geeigneten Maßnahmen zur Qualitätsverbesserung führen.

Literaturverzeichnis

[ALM99a] G. Almes, S. Kalidindi, and M. Zekauskas. A One-way Delay Metric for IPPM. http://www.rfc-editor.org/rfc/rfc2679.txt.

[ALM99b] G. Almes, S. Kalidindi, and M. Zekauskas. A One-way Packet Loss Metric for IPPM. http://www.rfc-editor.org/rfc/rfc2680.txt

[DC02] C. Demichelis and P. Chimento. IP Packet Delay Variation Metric for IP Performance Metrics (IPPM). http://www.rfc-editor.org/rfc/rfc3393.txt.

[DFN09] http://www.dfn.de/projekte/gefoerderte-projekte/.

[FAA] http://gps.faa.gov.

[GEA] The GÉANT Network. http://www.geant.net/.

[HAD09] http://www.win-labor.dfn.de/English/dienste_aktiv.html.

[HOL07] T. Holleczek: Redesign und Implementierung eines Softwarepakets zur Messung der IP Performance nach OWAMP-Standard. Studienarbeit, Universität Erlangen-Nürnberg, 2007.

[HOL08] T. Holleczek: Statistical Analysis of IP Performance Metrics in International Research and Educational Networks. Diplomarbeit, Universität Erlangen-Nürnberg, 2008.

[HKK06] P. Holleczek, R. Karch, R. Kleineisel, S. Kraft, J. Reinwand, and V. Venus. Statistical characteristics of active IP one way delay measurements. In R. Karch, editor, Proc. International Conference on Networking and Services, ICNS ’06, pages 1–1, 2006.

[NTP1] http://de.wikipedia.org/wiki/Network_Time_Protocol.

[NTP2] http://tools.ietf.org/html/rfc1305.

[PAMM98] V. Paxson, G. Almes, J. Mahdavi, and M. Mathis. Framework for IP Performance Metrics. http://www.rfc-editor.org/rfc/rfc2330.txt.

[XWI] X-WiN – Germany’s National Research and Educational Network. http://www.dfn.de/content/xwin.

perfSONAR-Lite TSS: Schnelldiagnose von Netzverbindungen im EGEE-III-Projekt

Susanne Naegele-Jackson[*], Martin Gründl[*], Andreas Hanemann[#]

[*] Friedrich-Alexander Universität Erlangen-Nürnberg
Martensstrasse 1, 91058 Erlangen
{susanne.naegele-jackson, martin.gruendl}@rrze.uni-erlangen.de

[#] DFN-Verein
Alexanderplatz 1, 10178 Berlin
hanemann@dfn.de

Zusammenfassung: Das EGEE-III-Projekt (Enabling Grids for E-sciencE) vernetzt mehr als 280 Einrichtungen in Europa und ist damit eines der führenden Grid-Projekte. Es ist daher notwendig, eine Lösung zur Fehlersuche auf der Netzebene zu haben, falls die Eigenschaften von Verbindungen über das Netz nicht wie erwartet sind. Im Vorgängerprojekt EGEE-II wurde hierzu eine eigene Monitoring-Lösung entwickelt, die jedoch von den Einrichtungen in großer Mehrheit als zu aufwendig im Betrieb betrachtet wurde. Deshalb wurde diese Lösung verworfen und in EGEE-III ein Troubleshooting-Ansatz gewählt, bei dem nur bei aktuellen Problemen eine leicht zu handhabende Untersuchungssoftware eingesetzt wird. Diese am RRZ Erlangen entwickelte Software basiert auf Teilen des im GN2/GN3-Projekt entwickelten Monitoringsystems perfSONAR.

1 Einleitung

Das EGEE-III-Projekt [EGEE] ging aus den Projekten EGEE-I und EGEE-II hervor und baut auf den Erfahrungen dieser Projekte auf. Die Überwachung und Fehlersuche im Gesamtnetz stellte sich im Laufe der ersten beiden Projekte immer mehr als komplexe Aufgabe dar. Zu Beginn von EGEE-III wurde zunächst innerhalb der EGEE-SA1 Activity eine Lösung zur Netzüberwachung angestrebt. Es zeigte sich dann allerdings, dass ein solches komplettes Monitoring über das ganze Netz, welches mehr als 40 Netzbetreiber umfasst, viel zu komplex für einen dauerhaften Einsatz und eher ungeeignet für die Schnelldiagnose von Problemen war. Außerdem standen viele NRENs (National Research and Education Networks) und Grid Partner einer allumfassenden Netzüberwachung mit fremdkontrolliertem Verkehr eher abneigend gegenüber, da sie das Netz in erster Linie für Projektaufgaben verwenden und nicht durch Verkehr für aktive Messungen belasten wollen.

Um trotzdem effizient und schnell nach Problemen im Netz suchen zu können, war die Alternative zum Netzmonitoring die Entwicklung von Troubleshooting Tools, mit deren Hilfe man Verbindungsprobleme gezielt aufspüren und dadurch schneller lösen kann. Verbindungstests sollten möglich sein, die nicht von einem zentralen Router aus durchgeführt werden, sondern direkt über die betroffenen Routen die Schwachstelle untersuchen können. Dabei sollten die Untersuchungen einer Netzstörung nicht dadurch behindert werden, dass die Tests zur Problemdiagnose nicht sofort durchgeführt werden können. Ein Netzadministrator soll keine wertvolle Zeit dadurch verlieren, dass er nach Accounts und Hosts auf beiden Seiten der gestörten Strecke suchen muss, sondern soll durch eine einfache Konfiguration von Diagnosetests unterstützt werden.

Aus diesem Hintergrund heraus ergaben sich folgende Anforderungen an ein neues Netzdiagnosesystem: Es sollte unbedingt eine „light-weight“ Lösung sein, die nicht unnötig durch permanenten Testverkehr rund um die Uhr Bandbreite in Anspruch nimmt. Mit anderen Worten, es sollte eine Troubleshooting Lösung entwickelt werden, die gezielt bei einem Problem „on-demand“ eingesetzt werden kann. Außerdem sollte die Lösung möglichst leicht weiträumig verteilt werden können und plattformunabhängig der großen Anzahl von Nutzern in der EGEE Grid Community zur Verfügung gestellt werden können. Eine weitere Anforderung war, dass es sich bei den Modulen um nachhaltige Entwicklungen handeln sollte, und sofern möglich, auf bereits vorhandener und im Einsatz verbreiteter Software aufsetzen sollte. Dieses Kriterium führte dazu, dass das weitverbreitete perfSONAR (siehe unten) und dessen Kommunikationsschnittstelle in die neue Troubleshooting Software integriert wurde und damit „perfSONAR-Lite TSS (Troubleshooting Service)“ entstand.

2 perfSONAR und verwandte Arbeiten

Für das Netzmonitoring existieren bereits viele einzelne Tools wie z.B. MRTG [MRTG] oder iperf [IPERF] sowie komplette Lösungen. Für das Monitoring von Clustern oder Grids kann beispielsweise Ganglia [Ganglia] eingesetzt werden, während MonALISA [MonALISA] zum Netzmonitoring mit Agenten geeignet ist. Es liegt daher nahe eine Lösung für Troubleshooting in EGEE als Erweiterung einer schon existierenden Software zu entwickeln. Das für Multi-Domain Umgebungen entwickelte perfSONAR eignet sich für diesen Zweck, da es durch seine modulare Architektur und Flexibilität hinsichtlich der Meßmethoden leicht angepasst werden kann. Dieses wurde auch bereits mit dem Tool Command-Line MP [SKCM07] vom brasilianischen Forschungsnetz RNP gezeigt. Dieses ist jedoch nur zur Messung von Durchsatz (Tool BWCTL, [BWCTL]), Verzögerung (Tool OWAMP, [OWAMP]), Ping und Traceroute geeignet und kann nicht so einfach an die im EGEE-Projekt zu beachtenden Rahmenbedingungen hinsichtlich der Beschränkungen der Nutzerrechte angepasst werden.

perfSONAR (Performance focused Service Oriented Network Monitoring Architecture) [perfSONAR, BBDH05, HKMR08] ist eine dienstorientierte Architektur für multi-domain Netzüberwachungen und Störungsdiagnose, die im GN2 bzw. GN3-Projekt [GN2/GN3] sowie von internationalen Partnern wie z.B. Internet2 entwickelt wurde bzw. wird. Netzadministratoren können mit Hilfe dieses Tools Engpässe im Netz auch außerhalb ihrer Domains frühzeitig erkennen und Ende-zu-Ende Probleme leichter und schneller lösen. perfSONAR ist aber als Netzüberwachungssystem konzipiert und nicht speziell für Troubleshooting geeignet.

In perfSONAR werden drei Schichten unterschieden (s. Abbildung 1): Der Measurement Point Layer, der Service Layer und der User Interface Layer. Im Measurement Point Layer werden aktive oder passive Messungen mit Hilfe von verschiedenen Netzüberwachungswerkzeugen über sogenannte Measurement Points (MPs) durchgeführt. Ein MP ist dabei jeweils für eine Art von Netzkennzahlen konzipiert, z.B. für Auslastung, Paketlaufzeiten oder Paketverluste. Der Service Layer dient zum Management der Messungen und gliedert diese Aufgaben in spezifische Web Services. Beispielsweise gibt es Dienste zur Archivierung von Messungen, zur Suche nach Messungen oder anderen Diensten und für die Autorisierung bei der Durchführung von Messungen. Im User Interface Layer werden schließlich mehrere Visualisierungswerkzeuge angeboten, die den Zugriff auf die Messdaten erlauben.

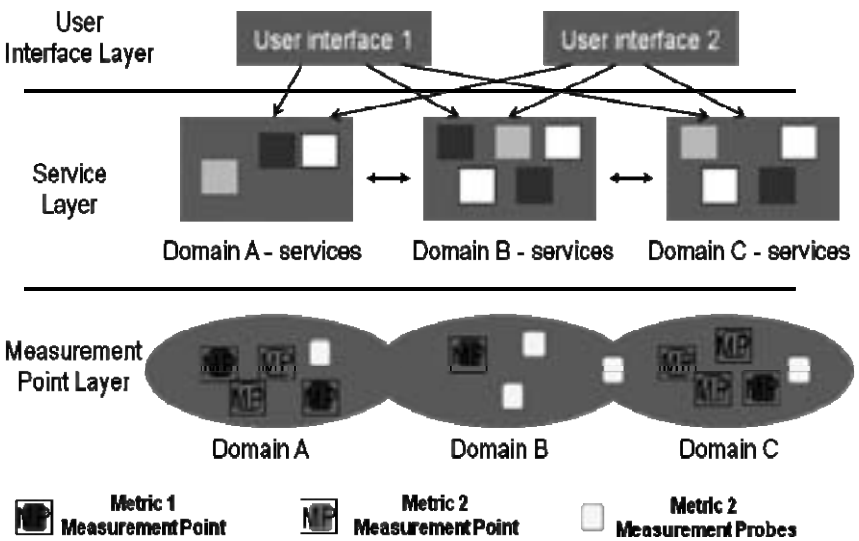


Abbildung 1: Das Drei-Schichten-Modell von perfSONAR

perfSONAR basiert auf der Web Services Technologie, so dass der Austausch zwischen den einzelnen Services über die Extensible Markup Language (XML) klar definiert ist. Ein besonderer Schwerpunkt von perfSONAR sind IP-Metriken: Verfügbarkeitsdaten, die die Robustheit eines Netzes beschreiben, sowie Verlustraten und Fehlerraten, die auf mögliche Staus im Netz oder auf Gerätefehler hinweisen, und auch Latenzdaten, die überlastete Verbindungen oder eventuelle Umleitungen über andere Routen aufzeigen.

perfSONAR wird zurzeit im LHC OPN (privates optisches Netz für das Large Hadron Collider Projekt am CERN, [LHC OPN]) und im GÉANT Netz eingesetzt, außerdem wird es auch bei vielen NRENs verwendet. Die Entwicklung der Troubleshooting Tools auf dieser weitverbreiteten Software aufzusetzen, ist daher nicht nur sinnvoll, sondern ermöglicht auch eine schnelle Akzeptanz von Nutzerseite.

3 PerfSONAR-Lite Troubleshooting Tools

Das DFN-Labor in Erlangen entwickelt für perfSONAR im Rahmen des GN2/GN3-Projektes einen speziellen Mess-PC für die aktive Messung von Paketlaufzeiten, deren Schwankungen, Paketverlusten sowie den Netzpfaden. Diese Messstationen werden an interessanten Stellen im Netz, z.B. den GÉANT PoPs, aufgestellt. Deren Messdaten werden archiviert und über eine perfSONAR-Schnittstelle bereitgestellt. Desweiteren wird für das von Internet2 stammende Tool BWCTL (Bandwidth Test Controller, [BWCTL]) eine perfSONAR-Schnittstelle zur Verfügung gestellt.

Die durch dieses Projekt vorhandene perfSONAR-Kommunikationsschnittstelle ist der Ausgangspunkt für die Implementierung im EGEE-III-Projekt. Sie ist für die Verwendung von mehreren Test Tools so erweitert worden, dass die Ergebnisse der Tests über die perfSONAR-Schnittstelle bereit stehen. Für die Tools, die integriert werden sollen, gab es von EGEE die Vorgabe, dass mindestens Ping, Traceroute, BWCTL, Port Scan (Tool NMAP, [NMAP]) sowie DNS Lookup unterstützt werden sollen. Die Metriken wurden so ausgewählt, damit sie für möglichst viele Anwendungen relevant sind und dass das Troubleshooting anwendungsübergreifend zum Einsatz kommen kann. Die Test Tools zusammen mit der perfSONAR-Schnittstelle sind für die einfache Installation und Verwendung im Problemfall bei einer oder mehrerer EGEE-Sites geeignet. Die Web-basierte Software steht auf einem vom zentralen EGEE Network Operation Center (ENOC) betriebenen Webserver für alle registrierten Benutzer bereit.

Das typische Szenario (siehe Abbildung 2) sieht so aus, dass bei einem Netzproblem zwischen Netzknotenpunkten A und B ein Netzwerkadministrator mit den erforderlichen Zugangsrechten von einem entfernten Netzknotenpunkt (d.h. dem ENOC) aus die Tools von Punkt A oder B für eine Ferndiagnose starten und so die Strecke zwischen A und B untersuchen kann. Selbst beim DNS Lookup Service kann dies von Vorteil sein, insbesondere dann, wenn eine Abfrage zu einem internen Host über einen lokalen DNS Server detailliertere Informationen liefern kann als über eine globale DNS-Abfrage von außen zur Verfügung gestellt wird.

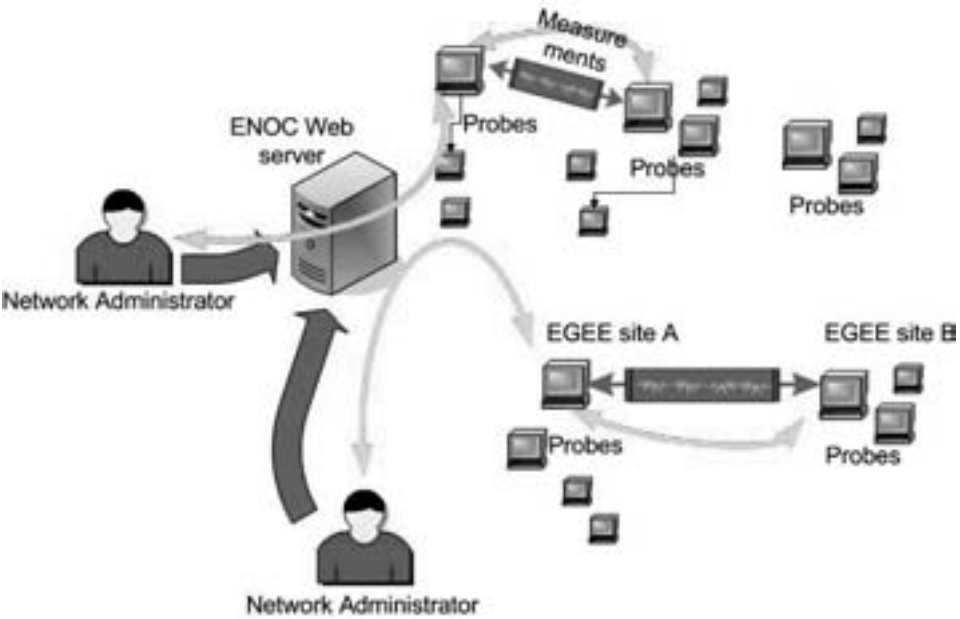


Abbildung 2: Einsatz der Troubleshooting Service Tools für Ferndiagnosen

Die eigentliche Ausführung der perfSONAR-Lite TSS (Troubleshooting Service) Tools erfolgt über die plattform-unabhängige perfSONAR-basierte Plugin Architektur, die in Abbildung 3 dargestellt ist: Grundelement dieser Architektur ist ein generisches Plugin, über das die Service-Anfragen aktiviert werden. Dabei handelt es sich um ein XML-Template, das mit den Abfrageparametern des Benutzers ergänzt wird. Die vollständige XML-Nachricht wird dann in einen SOAP (Simple Object Access Protocol) Envelope verpackt und kann so als strukturierte Information an das perfSONAR Interface übergeben werden. Nach Ausführung der Anfrage mit eventueller Durchführung einer Messung liefert das perfSONAR-Kernmodul die Ergebnisse zurück, so dass sie dem Benutzer über die perfSONAR-Lite TSS Schnittstelle zur Verfügung gestellt werden können.

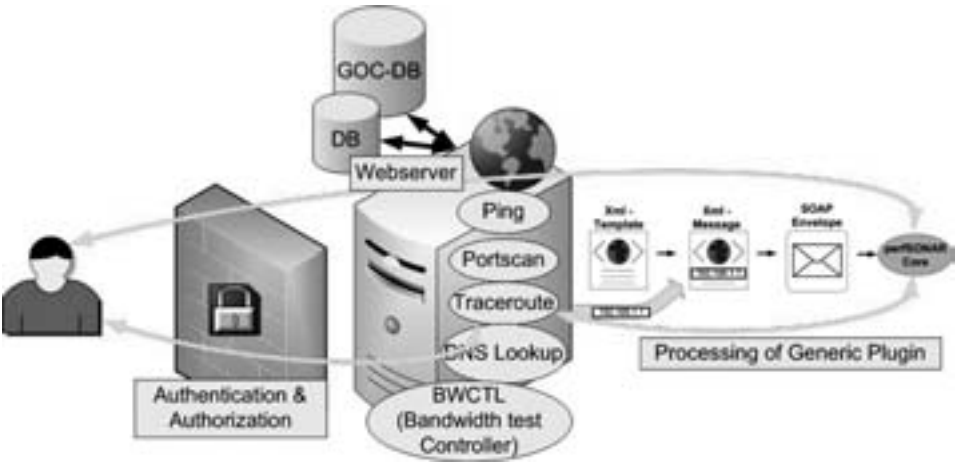


Abbildung 3: perfSONAR-Lite TSS Messungen in einer EGEE Site

Alle Messanfragen werden über die Benutzerschnittstelle auf dem ENOC Webserver gestartet. Aber der Webserver liefert nicht nur das Interface, wo ein Nutzer Service-Anfragen stellen kann, sondern ist auch verantwortlich für Authentifizierung und Autorisierung der Anwender.

Der Zugang zu den Messungen ist in einem Drei-Schichten-Modell geregelt, welches in Abbildung 4 gezeigt wird: Auf der höchsten Ebene stehen die Super User vom ENOC, die grundsätzlich jede Messung von jedem Start- und Zielpunkt aus aufrufen können. Die zweite Ebene bilden sogenannte Managers, die über die GOC-DB (Grid Operations Center Database) definiert sind; typischerweise sind Manager Benutzer, die in der GOC-DB Rollen wie z.B. „Regional Manager“, „Site Administrator“ oder „Deputy Regional Manager“ belegen. Die Granularität eines Managerzugangs zum Messbereich beschränkt sich auf Standorte, wobei jeder Standort („site“) beliebig viele Messstationen („probes“) betreiben kann. Manager, die einem ROC (Regional Operations Center) angehören, haben üblicherweise Zugang zu allen Messstationen dieses ROCs. Die Zugehörigkeit eines Managers zu einem ROC oder zu einem Standort wird über die GOC-DB verifiziert. Die dritte Ebene der Zugangskontrolle betrifft normale Benutzer: Grundsätzlich kann sich jeder als Nutzer registrieren lassen, solange er über ein gültiges Gridzertifikat verfügt, das von einer gültigen Certificate Authority (CA) ausgestellt wurde und nicht wegen einem Missbrauch entzogen wurde. Allerdings muss er sich zusätzlich von einem Manager als Nutzer registrieren lassen. Ein Manager kann Benutzerregistrierungen bequem über die Management-Plattform auf dem Webserver durchführen; über diese Plattform kann ein Manager auch Messstationen registrieren und verwalten. Die Zugangsgranularität für Benutzer auf Ebene 3 erlaubt eine Zugangsbeschränkung einzelner Benutzer auf individuelle Messstationen.

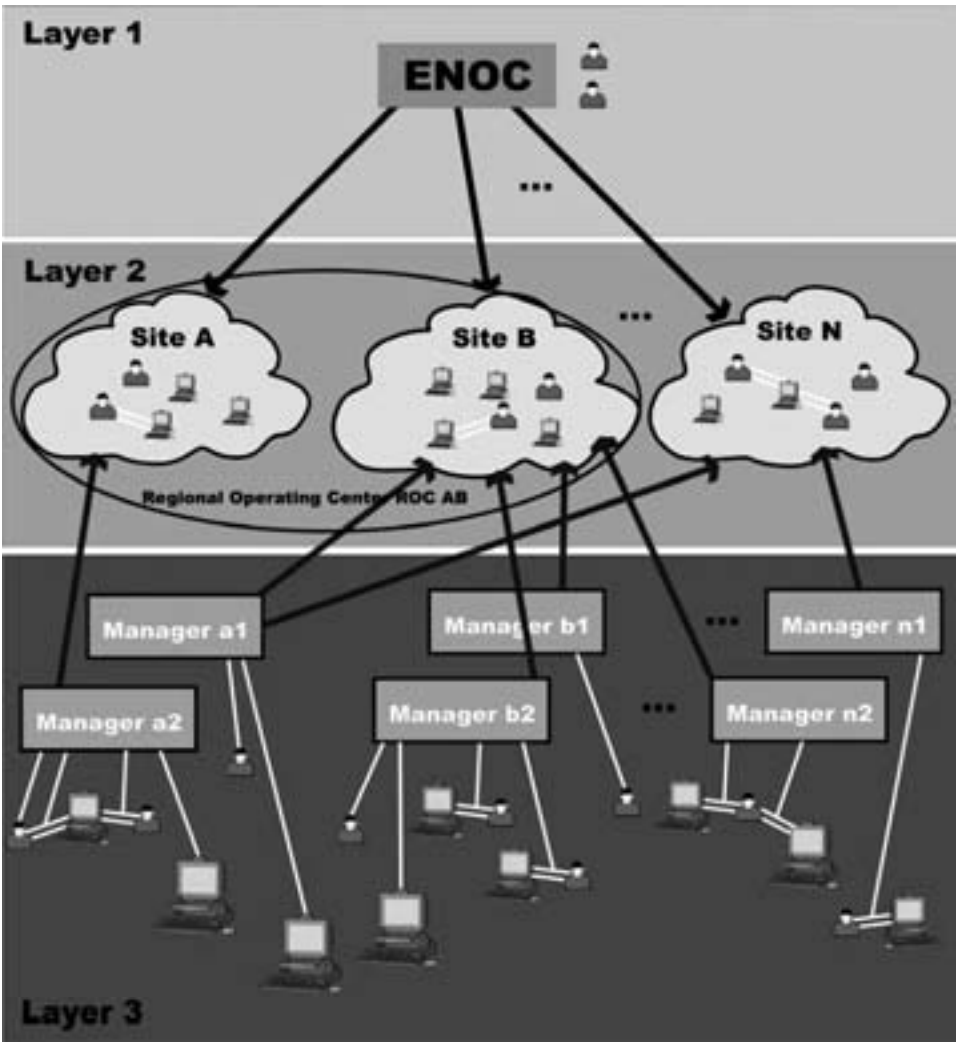


Abbildung 4: 3-Schichtenmodell für Autorisierung und Authentifizierung

Um eine Abfrage oder Messung von einer Messstation starten zu können, muss dort ein perfSONAR-Lite TSS Client installiert werden. Für die Kommunikation zwischen Client und Webserver wird eine SSL-Verbindung aufgebaut. Messungen sind grundsätzlich erlaubt, wenn der Benutzer Zugangsrechte auf eine Messstation hat, die entweder Start- oder Zielpunkt der Abfrage ist. Bei jeder Messung wird der Manager, der die betreffende Messstation über die Management Plattform registriert hat, über die Messanfrage mit einer E-Mail informiert, die Aussagen liefert zu Start- und Zielpunkt der Messung und Art der durchgeführten Anfrage. Beim Service Tool Port-scan wird der Manager auch über weitere Angaben wie z.B. betroffene Einzelports oder Portbereiche informiert.

Abbildung 5 zeigt die Durchführung eines BWCTL-Tests zwischen zwei EGEE Sites durch das ENOC. Hierbei wird ein Test mit TCP 20 Sekunden lang durchgeführt und man erhält das übertragene Gesamtvolumen sowie die durchschnittliche Geschwindigkeit. Die Parameter Window Size und Round Trip Time (RTT) wurden im konkreten Fall von BWCTL selbst bestimmt, wobei auch externe Vorgaben möglich sind. Eine graphische Darstellung der Ergebnisse wird derzeit entwickelt.

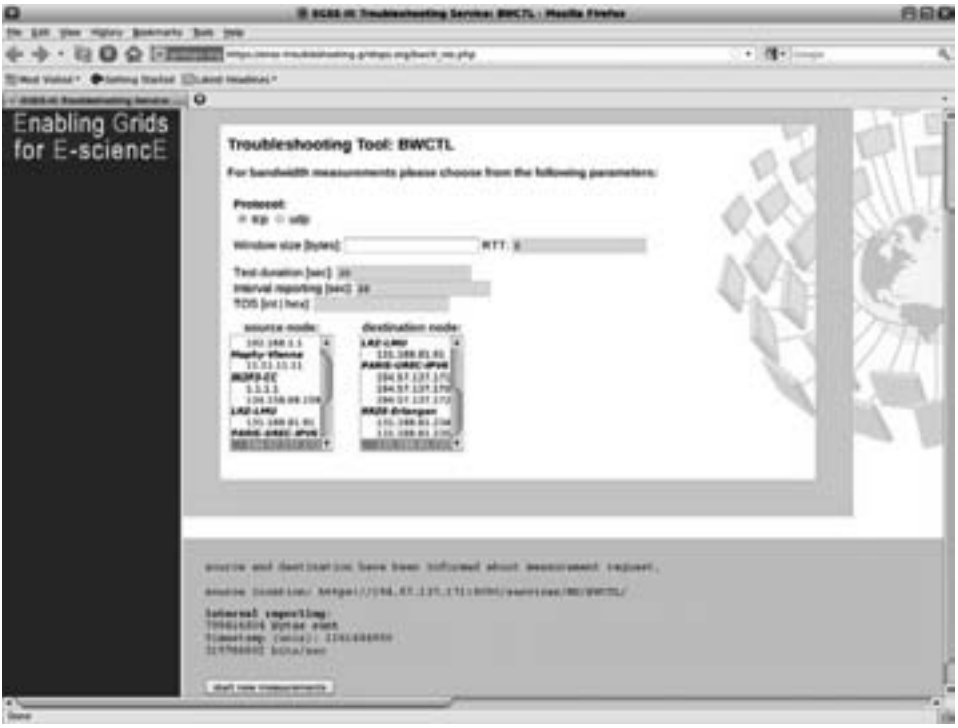


Abbildung 5: Verwendung von BWCTL in der Serveranwendung von perfSONAR-Lite TSS

4 Einsatz im EGEE-Projekt und darüber hinaus

Wie im vorherigen Abschnitt darstellt, wurde die Software für das EGEE-III-Projekt entwickelt und wird nun in Kürze für das Troubleshooting entsprechend dem EGEE-Betriebskonzept eingesetzt. Die Software ist derzeit teilweise an den Bedingungen des EGEE-III-Projekts ausgerichtet, insbesondere was das Rechtemanagement angeht, wo eine Kopplung mit den entsprechenden Datenbanken erfolgte. In weiten Teilen, d.h. im Bezug auf die Troubleshooting Tools selbst sowie die Kommunikation mit perfSONAR-Interface, ist die Software jedoch auch für allgemeinere Szenarien geeignet.

Beispielsweise könnte bei einem Projekt wie dem Large Hadron Collider am CERN ein permanentes Monitoring für das Kernnetz (hier die Kopplung von Tier0 und Tier1-Zentren) gewünscht werden. Für die Zusammenarbeit mit Tier2-Zentren oder spätestens für die Verbindungen mit Tier3-Zentren wären diese Lösungen aber recht aufwendig, so dass sich eine leicht zu installierende Troubleshooting-Lösung anbietet.

Auch innerhalb des X-WiN sollte der Einsatz überlegt werden, so dass das DFN-NOC dieses Tool bei Bedarf zum Messen der Verbindung zu einer Einrichtung oder zwischen zwei Einrichtungen einsetzen könnte.

5 Zusammenfassung und Ausblick

Nachdem perfSONAR-Lite TSS seit Mai 2008 entwickelt wurde, konnte bei der EGEE-Konferenz in Barcelona im September 2009 eine Version der Software sowohl mit einem Vortrag als auch mit einer Demonstration vorgestellt werden. Die Software steht nun auch zum ausführlichen Testen für alle Teilnehmer am EGEE-Projekt bereit.

Zusätzliche Erweiterungen der Software sind geplant und werden insbesondere Archivierungsmöglichkeiten und erweiterte Darstellungen der Resultate betreffen. Außerdem wird zur Zeit noch an zusätzlichen Firewall-Regelungen für BWCTL-Tests gearbeitet; es soll dabei auch untersucht werden, wie es sich vermeiden lässt, dass Messungen fälschlicherweise von Intrusion Detection Systems (IDS) als DoS-Attacken interpretiert werden können.

Literaturverzeichnis

[BBDH05] Boote, J. W., Boyd, E. L., Durand, J., Hanemann, A., Kudarimoti, L., Lapacz, R., Swany, D. M., Zurawski, J., Trocha, S., PerfSONAR: A Service Oriented Architecture for Multi–Domain Network Monitoring, In *Proceedings of the Third International Conference on Service Oriented Computing*, 241–254, LNCS 3826, Springer Verlag, ACM Sigsoft, Sigweb, Amsterdam, The Netherlands, Dezember, 2005.

[BWCTL] http://e2epi.internet2.edu/bwctl/

[EGEE] http://www.eu-egee.org/

[Ganglia] http://ganglia.sourceforge.net/

[GN2/GN3] http://www.geant2.net/, http://www.geant.net

[HKMR08] Hanemann, A., Kraft, S., Marcu, P., Reinwand, J., Reiser, H., Schmitz, D., Venus, V., perfSONAR: Performance Monitoring in europäischen Forschungsnetzen, In *Proceedings Erstes DFN–Forum Kommunikationstechnologien — Verteilte Systeme im Wissenschaftsbereich*, GI–Verlag/DFN, Kaiserslautern, Deutschland, Mai, 2008.

[IPERF] http://iperf.sourceforge.net/

[LHC OPN] Large Hadron Collider Optical Private Network, http://lhcopn.web.cern.ch/lhcopn/

[MonALISA] MONitoring Agents using a Large Integrated Services Architecture, http://monalisa.caltech.edu/monalisa.htm

[MRTG] Multi Router Traffic Grapher, http://oss.oetiker.ch/mrtg/

[NMAP] http://nmap.org/

[OWAMP] http://www.internet2.edu/performance/owamp/

[perfSONAR] http://www.perfsonar.net/, http://wiki.perfsonar.net/

[SKCM07] Sampaio, L., Koga, I., Costa, R., Monteiro, H., Vetter, F., Fernandes, G., Vetter, M., Monteiro, J., "Implementing and Deploying Network Monitoring Service Oriented Architectures: Brazilian National Education and Research Network Measurement Experiments", Proceedings of the 5th Latin American Network Operations and Management Symposium (LANOMS 2007), Brazil, September 2007.

Ansätze zur Steigerung der Verfügbarkeit in Wissenschaftsnetzen

Christian Grimm, Sibylle Schweizer-Jäckle, Stefan Piger

DFN-Verein
Alexanderplatz 1
D-10178 Berlin
{grimm|schweizer|piger}@dfn.de

Abstract: Wissenschaftsnetze leisten einen wichtigen Beitrag zur Sicherung von Standortfaktoren im internationalen Wettbewerb von Wissenschaft und Forschung. Trotz eingeschränkter finanzieller Möglichkeiten ist es notwendig, den Anwendern eine störungsfreie Netzplattform zur Verfügung zu stellen. Am Beispiel des vom DFN-Verein für die deutsche Wissenschaft organisierten Wissenschaftsnetzes X-WiN werden mögliche Ansätze zur Steigerung der Verfügbarkeit auf verschiedenen Ebenen der Netzwerktechnik betrachtet. Mit diesen Maßnahmen wird im Wissenschaftsnetz derzeit eine Verfügbarkeit des DFNInternet-Dienstes von bis zu 99,999% erreicht.

1 Einleitung

Um am globalen Verbund wissenschaftlicher Kooperationen teilhaben zu können, verfügen weltweit alle technologisch entwickelten Nationen über speziell auf die Wissenschaft zugeschnittene Wissenschaftsnetze oder streben – je nach eigenem Entwicklungsstand – deren Aufbau an. Wissenschaftsnetze haben die Zielsetzung, wissenschaftliches Arbeiten zu unterstützen und sind mittlerweile ein integraler Bestandteil der zugehörigen Arbeitsprozesse in Forschung und Lehre. Hierfür müssen sie sich an den spezifischen organisatorischen und strukturellen Randbedingungen und den Bedarfen ihrer Anwender aus dem Wissenschaftsbereich orientieren.

Aufgrund ihrer zentralen Bedeutung für Wissenschaft und Forschung stellen Wissenschaftsnetze bereits heute eine kritische Infrastruktur dar. Dabei ist zu beachten, dass deren Wert gegenwärtig nicht mit Ansätzen wie im kommerziellen Bereich kalkuliert werden kann. So wird dem potentiellen Ausfall eines Wissenschaftsnetzes bisher kein konkreter wirtschaftlicher Schaden gegenüber gestellt, wie es etwa bei Störungen in den IT-Infrastrukturen von z. B. Banken oder Versicherungen längst der Fall ist. Dennoch kommt der Sicherung eines stabilen und zuverlässigen Betriebes auch von Wissenschaftsnetzen eine stetig wachsende Bedeutung zu, insbesondere bei der Unterstützung internationaler Großforschungsprojekte wie in der Hochenergie- (z. B. Large Hadron Collider, LHC) oder Astrophysik (z. B. Low Frequency Array, LOFAR). Hierbei gilt es, trotz eingeschränkter finanzieller Möglichkeiten den – unter anderem wegen Wartungsarbeiten z. T. auch unabdingbaren – Unterbrechungen durch geeignete technische Maßnahmen entgegenzuwirken, um aus Sicht der Anwender einen störungsfreien Betrieb zu gewährleisten.

Im Folgenden werden Aspekte der Verfügbarkeit am Beispiel des vom DFN-Verein für die deutsche Wissenschaft organisierten Wissenschaftsnetzes X-WiN erörtert. Hierfür werden zunächst die grundsätzlich möglichen Ebenen diskutiert, auf denen sich in komplexen Netzinfrastrukturen Ansätze zur Verbesserung der Verfügbarkeit bieten. Danach werden die verschiedenen technischen Ebenen des X-WiN und entsprechende Maßnahmen zur Steigerung der Verfügbarkeit vorgestellt. Den Abschluss bildet eine Evaluation der getroffenen Maßnahmen, basierend auf aktuellen Messungen und Verfügbarkeitsstatistiken aus dem X-WiN.

2 Verfügbarkeit

Grundsätzlich bezeichnet Verfügbarkeit die Wahrscheinlichkeit, dass ein System zu einem betrachteten Zeitpunkt t betriebsfähig ist, d. h. gemäß einer vorgegebenen Spezifikation korrekt arbeitet [BP75]. Sie berechnet sich damit nach der einfachen Formel

$$V = (Gesamtzeit - Gesamtausfallzeit) / Gesamtzeit$$

Daraus folgt, dass sich Angaben zur Verfügbarkeit grundsätzlich auf einen beobachteten Zeitraum beziehen. Differenziertere Betrachtungen der Verfügbarkeit unterscheiden zwischen den Ursachen für die Ausfälle. Die häufig verwendeten inhärenten und erreichbaren Verfügbarkeiten beziehen sich auf Ausfälle innerhalb des betrachteten Systems, sei es verursacht durch fehlerhafte Bauteile oder auch Konfiguration. Im Gegensatz dazu schließt die operationale Verfügbarkeit jegliches Fehlverhalten, d. h. auch Ausfälle verursacht durch äußere Einwirkungen wie Stromausfall, ein: „Die operationale Verfügbarkeit A_0 einer Betrachtungseinheit ist die Wahrscheinlichkeit, dass die Betrachtungseinheit alle zugesicherten Eigenschaften bei den beschriebenen Umgebungsbedingungen einhält oder fehlerfrei funktioniert.“ [BSI09].

Objektive Fakten bilden die Grundlage jeglichen Diskurses im wissenschaftlichen Umfeld, dies gilt sowohl bei der Publikation wissenschaftlicher Ergebnisse als auch bei der Prüfung und Bewertung technischer Infrastrukturen. Daher wird im Folgenden aus mehreren Gründen ausschließlich die operationale Verfügbarkeit betrachtet:

- Die operationale Verfügbarkeit lässt sich eindeutig und mit geringem Aufwand messen, da nicht nach der Ursache für die Ausfälle unterschieden werden muss.

- Die operationale Verfügbarkeit lässt sich auch von den Anwendern geeignet prüfen, da sie der tatsächlich „wahrgenommenen“ Verfügbarkeit entspricht.

- Die operationale Verfügbarkeit stellt die untere Grenze bzw. den ungünstigsten Wert der Verfügbarkeit dar. Die Angabe besserer Werte wie z. B. der inhärenten Verfügbarkeit müsste stets mit der expliziten Beschreibung der betrachteten Umgebung sowie der Art der berücksichtigten Ausfälle einhergehen, um eine Vergleichbarkeit und Reproduzierbarkeit der Ergebnisse gewährleisten zu können [PH01].

Im Folgenden werden die Betrachtungen zur Verfügbarkeit der Netzinfrastruktur am Beispiel des vom DFN-Verein für die deutsche Wissenschaft organisierten Wissenschaftsnetzes X-WiN erörtert.

3 Die Netzplattform im Wissenschaftsnetz

Das Wissenschaftsnetz X-WiN ist die technische Plattform des Deutschen Forschungsnetzes. Über das X-WiN sind Hochschulen, Forschungseinrichtungen und forschungsnahe Unternehmen in Deutschland untereinander, mit den Wissenschaftsnetzen in Europa und auf anderen Kontinenten verbunden. Darüber hinaus verfügt das X-WiN über leistungsstarke Austauschpunkte mit dem allgemeinen Internet.

Mit Anschlusskapazitäten bis zu einem Mehrfachen von 10 Gbit/s pro Teilnehmereinrichtung und einem Terabit-Kernnetz, das sich zwischen ca. 60 Kernnetz-Standorten aufspannt, zählt das X-WiN zu den leistungsfähigsten Kommunikationsnetzen weltweit.

3.1 Optische Plattform

Mit dem Ende des Jahres 2005 erfolgten Übergang vom G-WiN zum X-WiN wurde das Wissenschaftsnetz von beschalteten Providerverbindungen auf eine *dark fibre* basierte, d. h. auf unbeschalteten Glasfaserstrecken gegründete Infrastruktur, umgestellt. Daraus resultiert die in Abbildung 1 dargestellte Glasfaserinfrastruktur aus derzeit 89 Einzelstrecken mit einer Gesamtlänge von etwa 10.000 km. Die Topologie des Kernnetzes wird im Wesentlichen aus mehreren Ringen gebildet, die zur Erhöhung der Redundanz einen z. T. deutlich höheren Vermaschungsgrad aufweisen. Damit ist bis auf wenige Ausnahmen, in denen keine redundant geführten Glasfaserstrecken zur Verfügung standen, sichergestellt, dass alle Kernnetzstandorte über mindestens zwei Wege erreichbar sind.

Auf dieser Infrastruktur aufbauend wurde eine optische Veredelung mit DWDM-Technik realisiert, die aktuell bis zu 40 Wellenlängenverbindungen mit einer maximalen Datenübertragungsrate von 10 Gbit/s je Glasfaserstrecke ermöglicht. Neben den für den DFNInternet-Dienst verwendeten Wellenlängen für Router-Verbindungen werden mit dieser Technik auch VPN-Verbindungen auf Layer 2 mit bis zu 10 Gbit/s zwischen Anwendern realisiert.

Die redundante Topologie des X-WiN bietet auch unmittelbar Möglichkeiten zur Erhöhung der Verfügbarkeit von VPN-Strecken auf Layer 2. So kommt bei Bedarf über vollständig disjunkte Alternativwege für nahezu alle Verbindungen zwischen Kernnetzstandorten eine als optische Protection bezeichnete Funktionalität der DWDM-Technik zum Einsatz.

Diese auch aus Netzen auf Basis von Sonet/SDH bekannte Funktionalität nutzt neben dem für den Normalbetrieb geschalteten so genannten Working-Path einen als Protection-Path bezeichneten Zweitweg. Auf diesen wird eine VPN-Strecke bei Ausfall des Working-Path innerhalb von 25 ms automatisch umgeschaltet, so dass selbst zeitkritische Anwendungen ohne Unterbrechung weiter ausgeführt werden können.

Abbildung 1: Topologie der optischen Plattform des X-WiN

3.2 IP-Plattform

Das in Abbildung 2 dargestellte Kernnetz des X-WiN besteht aus vier SuperCore-Standorten (Erlangen, Frankfurt, Hannover, Potsdam), die untereinander vollvermascht über zwei Wellenlängenverbindungen auf der optischen Plattform mit jeweils 2·10 Gbit/s verbunden sind. Über diese zentralen Knotenpunkte werden die Peerings mit anderen Providern, darunter z. B. das Netz der Deutschen Telekom AG redundant mit zweimal je 10 Gbit/s realisiert. Globale Uplinks in die USA erfolgen sogar über zwei verschiedene Provider Telia und Global Crossing mit jeweils 10 Gbit/s.

Über die 55 jeweils mindestens doppelt mit 10 Gbit/s (in wenigen Ausnahmen 1 Gbit/s) angebundenen Kernnetzstandorte werden schließlich die Anwendereinrichtungen an das X-WiN angeschlossen. Zwischen den wenigen Kernnetzstandorten, an denen keine Glasfasern verfügbar sind, kommen beschaltete Providerverbindungen zum Einsatz.

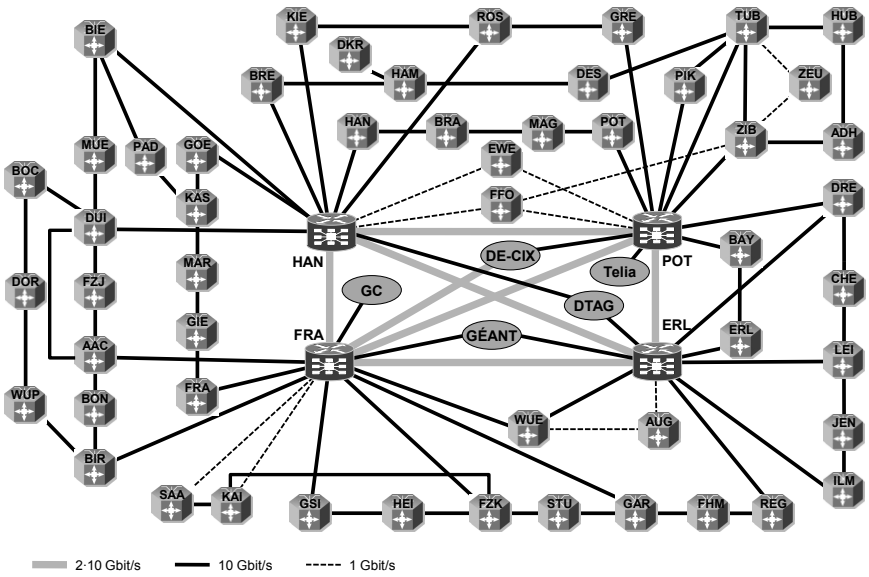


Abbildung 2: IP-Plattform des X-WiN

Durch angemessene Reduktion der unterstützten Anschlusstechniken und Einsatz neuer Geräte konnte auf IP-Ebene von vier Komponenten je Standort im G-WiN auf eine im X-WiN reduziert werden (Abbildung 3). Die verbleibende Netzkomponente ist dabei vollredundant hinsichtlich Stromversorgung, Routing Prozessoren und Interfaces. Im laufenden Betrieb können Hardware-Komponenten getauscht werden; Software Updates verursachen keine längeren Ausfallzeiten. Wartungsarbeiten lassen sich somit weitgehend ohne Beeinträchtigung des Betriebes durchführen.

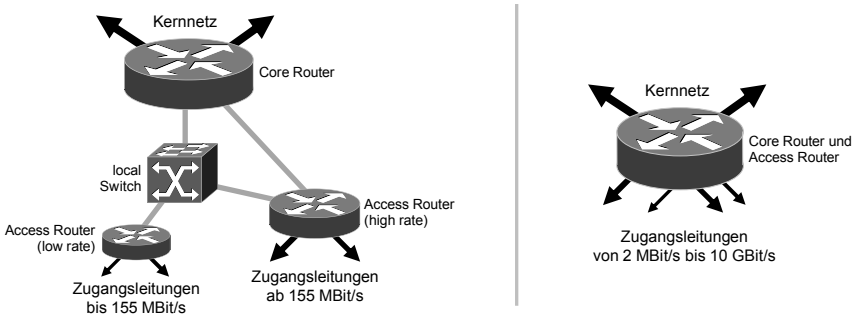


Abbildung 3: Vereinfachung der Kernnetzknoten vom G-WiN (links) zum X-WiN (rechts)

Der gezielte Einsatz von möglichst wenig verschiedenen technischen Komponenten an den Kernnetzstandorten erlaubt zusätzlich ein effizientes Ersatzteilkonzept und vereinfacht die Prozeduren zur Fehlersuche und Fehlerbehebung. Insgesamt 9 über Deutschland verteilte Ersatzteildepots ermöglichen den Ersatz von defekten Komponenten innerhalb von drei Stunden an jedem Kernnetzstandort.

3.3 Zugangsleitungen

Die oben ausgeführten Betrachtungen zur optischen und IP-Plattform zeigen, dass durch geeignete Topologie und Einsatz technischer Verfahren zur Überbrückung von Ausfällen Störungen im Kernnetz des Wissenschaftsnetzes weitgehend ohne Auswirkungen auf die Anwender bleiben. Weitaus kritischer zu bewerten sind jedoch die Zugangsleitungen zwischen den Einrichtungen und dem Kernnetz. Bisher war es üblich, die Einrichtungen lediglich über eine Zugangsleitung an einen Kernnetzstandort des Wissenschaftsnetzes anzubinden. Entsprechend einfach war es, mögliche Szenarien für Totalausfälle zu konstruieren. Hierbei ist zu berücksichtigen, dass bei auftretenden Störungen im Netz unmittelbar der gesamte Datenverkehr einer Einrichtung zum Erliegen kommt und dass häufig auch regulär anfallende Wartungsarbeiten zu Ausfällen führen. Entsprechend lag es nahe, Alternativen zur verbesserten Anbindung zu prüfen.

In Abbildung 4 sind die seit Anfang 2009 möglichen Anbindungen von Einrichtungen an das Wissenschaftsnetz dargestellt. Zu unterscheiden sind die Haupt- (durchgehende schwarze Linie) und Nebenleitungen (gestrichelte schwarze Linie) sowie Kunden-Router (KR), Cluster-Router (CR) und X-WiN-Router (XR).

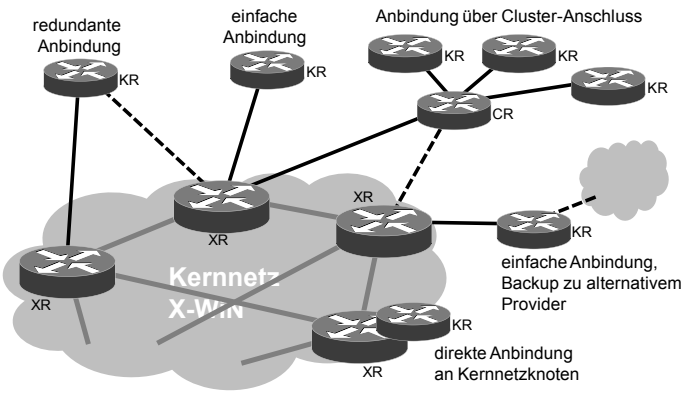


Abbildung 4: Anbindung von Einrichtungen an das Wissenschaftsnetz

Grundsätzlich sind damit fünf verschiedene Typen von Anbindungen möglich. Tabelle 1 fasst diese Typen zusammen und nennt die Häufigkeit der von Anwendern gewählten Anbindung im Wissenschaftsnetz mit Stand Ende 2009.

Entsprechend der Einteilung aus Tabelle 1 lassen sich für jeden Typ potentielle Ausfallszenarien formulieren (Tabelle 2). Hierbei wird unterstellt, dass ein XR stets durch mindestens eine Kernnetzleitung eine Verbindung zu dem gesamten X-WiN aufrecht erhalten kann. Wie die Ausführungen zur Verfügbarkeit der optischen Plattform im Kernnetz in Kapitel 4.1 zeigen, ist diese Annahme gerechtfertigt. Da sich die Kunden-Router und Cluster-Router in der administrativen Domäne der Einrichtungen und damit in deren Verantwortung befinden, sind sie von den folgenden Betrachtungen ausgenommen. Die Übersicht der kritischen Ausfälle in Tabelle 2 liefert somit identische Ergebnisse für redundante Anbindung und Anbindung über Cluster-Anschluss.

	Typ	Beschreibung	Anzahl
1	Einfache Anbindung	Eine Hauptleitung zwischen KR und XR	100
2	Redundante Anbindung	Eine Hauptleitung zwischen KR und XR sowie zusätzlich eine Nebenleitung zwischen KR und einem anderen XR	158
3	Direkte Anbindung an Kernnetzknoten	Diese Einrichtungen befinden sich direkt an einem Kernnetzknoten, die Zugangsleitungen bestehen in der Regel aus einer kurzen Verbindung zwischen zwei Verteilerschränken. Die redundante Anbindung wird implizit durch die Kernnetzleitungen an andere XR übernommen.	48
4	Anbindung über Cluster-Anschluss	Mehrere Einrichtungen teilen sich einen redundant angebundenen Cluster-Anschluss. Die Anbindung des KR an den CR wird von jeder Einrichtung selbstverantwortlich organisiert, d.h. hier ist nicht zwingend eine redundante Anbindung gegeben. Die derzeit 36 CR sind redundant an das Kernnetz angebunden.	114
5	Einfache Anbindung, Backup über alternativen Provider	Eine Hauptleitung zwischen KR und XR sowie zusätzlich Nebenleitung zwischen KR und alternativem Provider	59

Tabelle 1: Verteilung der Anbindungen an das Wissenschaftsnetz

	Typ	Kritische Ausfälle
1	Einfache Anbindung	• Zugangsleitung oder • XR
2	Redundante Anbindung	• Haupt- und Nebenleitung gleichzeitig oder • beide XR gleichzeitig oder • Hauptleitung und XR der Nebenleitung gleichzeitig oder • Nebenleitung und XR der Hauptleitung gleichzeitig
3	Direkte Anbindung an Kernnetzknoten	• lokale Verbindung zwischen KR und XR oder • XR
4	Anbindung über Cluster-Anschluss	• Haupt- und Nebenleitung gleichzeitig oder • beide XR gleichzeitig oder • Hauptleitung und XR der Nebenleitung gleichzeitig oder • Nebenleitung und XR der Hauptleitung gleichzeitig
5	Einfache Anbindung, Backup über alternativen Provider	• Zugangsleitung oder • XR oder • Anbindung an alternativen Provider

Tabelle 2: Typen von Anbindungen und kritische Ausfälle

Gleichzeitig mit der Etablierung der verschiedenen Anschlusstypen wurde auch die Verfügbarkeit der Einrichtungen aus dem Wissenschaftsnetz intensiver beobachtet. Ziel der Maßnahme ist neben der Erkennung von kritischen Netzsituationen besonders auch die Erfolgskontrolle der Bemühungen für die redundanten Anbindungen. Die Ergebnisse dieser Beobachtungen werden im folgenden Kapitel vorgestellt.

4 Messung der Verfügbarkeit

Nach den Ausführungen in Kapitel 2 zur operationalen Verfügbarkeit werden im Folgenden sämtliche Abweichungen von der spezifizierten Funktion des DFNInternet-Dienstes als Fehlverhalten definiert. Daraus folgt, dass neben z. B. Leitungsunterbrechung auch Fehlfunktionen der technischen Komponenten, Ausfälle durch fehlerhafte Konfiguration sowie Unterbrechungen durch Wartungsarbeiten in die Verfügbarkeit einbezogen werden. Weiterhin gehen auch Störungen in der Betriebsumgebung, wie z. B. Ausfälle der Stromversorgung oder Klimatisierung, die ein Versagen des betrachteten DFNInternet-Dienstes verursachen, in die Bewertung der Verfügbarkeit ein.

Zur Feststellung der Verfügbarkeit wird über die X-WiN-Router im Kernnetz kontinuierlich die Erreichbarkeit der Interfaces auf den Kunden-Routern, die an die Haupt- oder Nebenleitung angeschlossen sind, geprüft. Diese aktiven Messungen werden im Abstand von wenigen Sekunden durchgeführt. Führen drei aufeinander folgende Messungen zu einer Fehlermeldung, wird die Anbindung als fehlerhaft markiert. Somit kann die gemessene Verfügbarkeit zuverlässig mit einer Auflösung von Minuten im jeweils gewählten Beobachtungszeitraum angegeben werden.

4.1 Optische Plattform

Die in der optischen Plattform aufgetretenen Unterbrechungen von Januar bis September 2009 sind in Tabelle 3 aufgeführt. Es zeigt sich, dass sowohl die Summe der Unterbrechungen mit insgesamt 311 Stunden bzw. annähernd 13 Tagen als auch die Dauer der maximalen Unterbrechungen erheblich sind und den Einsatz redundanter Technologie unerlässlich machen. Aufgrund der oben dargestellten Topologie, einhergehend mit optischer Protection, bleiben diese Unterbrechungen jedoch nahezu ohne Auswirkung auf die Verfügbarkeit des DFNInternet-Dienstes.

Art	Anzahl	Dauer gesamt [h]	Dauer mittel [h]	Dauer maximal [h]
Störung	10	116	11,6	37,3
Wartung	34	195	5,7	13,0

Tabelle 3: Unterbrechungen der optischen Plattform im Wissenschaftsnetz

4.2 IP-Plattform

Tabelle 4 fasst Betriebs- und Störungsminuten für den DFNInternet-Dienst im Wissenschaftsnetz im Betriebszeitraum Januar bis September 2009 zusammen. Es wird hier bereits deutlich, dass mit der redundanten Anbindung eine erhebliche Steigerung der Verfügbarkeit einhergeht.

	Betrieb [min]	Störung [min]	mittl. Verfügbarkeit [%]	mittlere Ausfallzeit [min]
Einfach	149.471.881 (87,32%)	50.837 (99,12%)	99,966	133,70
Redundant	21.713.879 (12,68%)	452 (0,88%)	99,998	8,68
Gesamt	171.185.760 (100,00%)	51.289 (100,00%)	99,970	117,78

Tabelle 4: Betriebs- und Störungsminuten für DFNInternet-Dienst im Wissenschaftsnetz

Die in Tabelle 4 dargestellten Werte geben lediglich die aus den Messungen berechneten Mittelwerte bzw. Erwartungswerte wieder. Entscheidend für die einzelne Einrichtung ist jedoch die tatsächliche Verfügbarkeit. Daher kommt für die gewünschte Bewertung des Wissenschaftsnetzes der Verteilung der einzelnen Verfügbarkeiten eine weitaus höhere Bedeutung zu als die in der Tabelle 4 aufgeführten Mittelwerte. Das Diagramm in Abbildung 5 stellt die fallend sortierten Verfügbarkeiten aller an das Wissenschaftsnetz angeschlossenen Einrichtungen dar. Der kritische Bereich mit vergleichsweise geringer Verfügbarkeit befindet sich folglich im rechten Abschnitt des Diagramms. Der hohen Anzahl an weitgehend störungsfrei angebundenen Einrichtungen stehen wenige Einrichtungen mit zum Teil erheblichen Unterbrechungszeiten gegenüber.

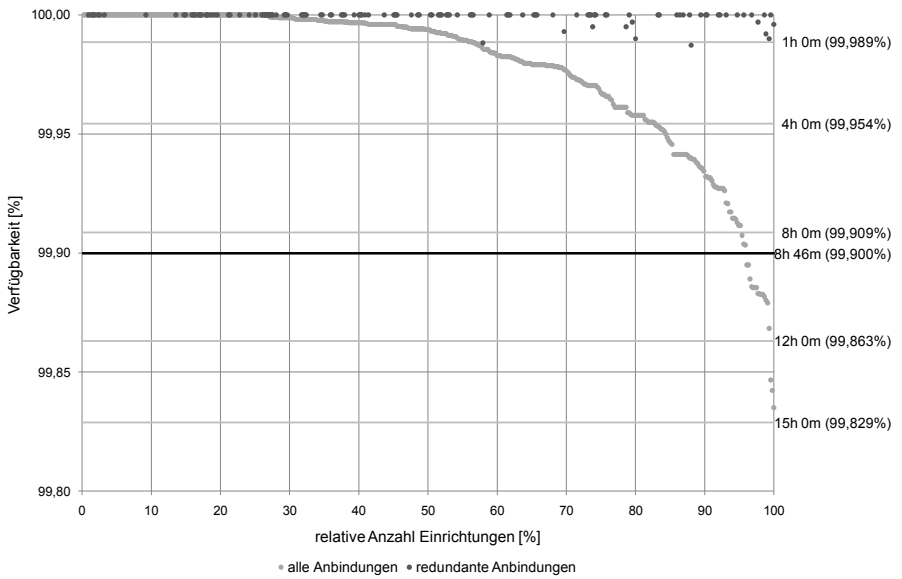


Abbildung 5: Verfügbarkeit aller an den DFNInternet-Dienst angebundenen Einrichtungen

Die dunklen Punkte in dem Diagramm kennzeichnen die Einrichtungen, die während des Beobachtungszeitraumes von der einfachen Anbindung auf die redundante Anbindung wechselten. Während die hellen Punkte die Beobachtungszeit von einfacher und redundanter Anbindung berücksichtigen, repräsentieren die dunklen Punkte ausschließlich den Zeitraum für die redundante Anbindung.

Aus dem Vergleich der Verteilungen für alle Anbindungen gegenüber den redundanten Anbindungen wird die Verbesserung durch die redundante Anbindung deutlich. Besonders im rechten Bereich des Diagramms sind erhebliche Steigerungen der Verfügbarkeit zu erkennen.

Die dargestellte Verteilung der redundant angebundenen Einrichtungen belegt somit noch deutlicher als Tabelle 4 den eindeutigen Gewinn. Nur in zwei Fällen wurde eine Ausfallzeit von einer Stunde (bzw. 99,989%) marginal überschritten. Nähere Untersuchungen zeigten darüber hinaus, dass nahezu sämtliche Störungen auf transiente Vorgänge während der Umschaltung von einfachem auf redundanten Betrieb zurückzuführen sind.

5 Zusammenfassung

Wissenschaftsnetze müssen sich einem in den letzten Jahren erheblich gestiegenen Anspruch an Leistungsfähigkeit und Verfügbarkeit stellen. Die vorgelegten Ergebnisse am Beispiel des DFNInternet-Dienstes zeigen, dass unter Zuhilfenahme neuester Netzwerktechnik und sorgfältiger Planung eine hohe Verfügbarkeit von bis zu 99,999% erreicht werden kann. Erforderlich sind jedoch erhebliche Anstrengungen auf allen Ebenen der Netzwerktechnologie, begleitet von funktionierenden Prozessen für das Fehlermanagement bis hin zur Ersatzteilversorgung.

Das Ziel einer unterbrechungsfreien Verfügbarkeit der Konnektivität wird mit den getroffenen Maßnahmen in beinah idealer Weise erreicht – die Erwartungen der Anwender an einen jederzeit funktionierenden DFNInternet-Dienst werden nahezu erfüllt. Eine weitere Steigerung ist nach derzeitigem Stand nur noch durch Änderungen an den eingesetzten Routing-Protokollen, insbesondere durch schnellere Reaktions- und Konvergenzzeiten, zu erzielen.

Abschließend sei bemerkt, dass die hohe Verfügbarkeit in Wissenschaftsnetzen nur dann einen erkennbaren Gewinn darstellt, wenn sie bis an die Nutzer weitergegeben werden kann. Eine entsprechende Qualität der Campusnetze ist daher unerlässlich. Hier müssen – sofern noch nicht geschehen –vergleichbare Anstrengungen unternommen werden. Dabei können die in diesem Beitrag vorgestellten Maßnahmen und Betrachtungen zur systematischen Analyse der bestehenden Verfügbarkeit aber auch zu deren Verbesserung als Vorbild und Leitfaden dienen.

Literaturverzeichnis

[BSI09] BSI: 1.2 Definitionen und Metriken für die Hochverfügbarkeit, Bundesamt für Sicherheit in der Informationstechnik, 2009

[BP75] Barlow, R.E.; Proschan, F.: Importance of system components and fault tree events, Stochastic Processes and their Applications, Elsevier, 1975; Vol. 3, Nr. 2, S. 153–173

[PH01] Piedad, F.; Hawkins, M.: High Availability – Design, Techniques and Processes; Prentice Hall, New Jersey, 2001

GI-Edition Lecture Notes in Informatics

P-1 Gregor Engels, Andreas Oberweis, Albert Zündorf (Hrsg.): Modellierung 2001.

P-2 Mikhail Godlevsky, Heinrich C. Mayr (Hrsg.): Information Systems Technology and its Applications, ISTA'2001.

P-3 Ana M. Moreno, Reind P. van de Riet (Hrsg.): Applications of Natural Language to Information Systems, NLDB'2001.

P-4 H. Wörn, J. Mühling, C. Vahl, H.-P. Meinzer (Hrsg.): Rechner- und sensorgestützte Chirurgie; Workshop des SFB 414.

P-5 Andy Schürr (Hg.): OMER – Object-Oriented Modeling of Embedded Real-Time Systems.

P-6 Hans-Jürgen Appelrath, Rolf Beyer, Uwe Marquardt, Heinrich C. Mayr, Claudia Steinberger (Hrsg.): Unternehmen Hochschule, UH'2001.

P-7 Andy Evans, Robert France, Ana Moreira, Bernhard Rumpe (Hrsg.): Practical UML-Based Rigorous Development Methods – Countering or Integrating the extremists, pUML'2001.

P-8 Reinhard Keil-Slawik, Johannes Magenheim (Hrsg.): Informatikunterricht und Medienbildung, INFOS'2001.

P-9 Jan von Knop, Wilhelm Haverkamp (Hrsg.): Innovative Anwendungen in Kommunikationsnetzen, 15. DFN Arbeitstagung.

P-10 Mirjam Minor, Steffen Staab (Hrsg.): 1st German Workshop on Experience Management: Sharing Experiences about the Sharing Experience.

P-11 Michael Weber, Frank Kargl (Hrsg.): Mobile Ad-Hoc Netzwerke, WMAN 2002.

P-12 Martin Glinz, Günther Müller-Luschnat (Hrsg.): Modellierung 2002.

P-13 Jan von Knop, Peter Schirmbacher and Viljan Mahni_ (Hrsg.): The Changing Universities – The Role of Technology.

P-14 Robert Tolksdorf, Rainer Eckstein (Hrsg.): XML-Technologien für das Semantic Web – XSW 2002.

P-15 Hans-Bernd Bludau, Andreas Koop (Hrsg.): Mobile Computing in Medicine.

P-16 J. Felix Hampe, Gerhard Schwabe (Hrsg.): Mobile and Collaborative Busi-ness 2002.

P-17 Jan von Knop, Wilhelm Haverkamp (Hrsg.): Zukunft der Netze –Die Verletzbarkeit meistern, 16. DFN Arbeitstagung.

P-18 Elmar J. Sinz, Markus Plaha (Hrsg.): Modellierung betrieblicher Informationssysteme – MobIS 2002.

P-19 Sigrid Schubert, Bernd Reusch, Norbert Jesse (Hrsg.): Informatik bewegt – Informatik 2002 – 32. Jahrestagung der Gesellschaft für Informatik e.V. (GI) 30.Sept.-3.Okt. 2002 in Dortmund.

P-20 Sigrid Schubert, Bernd Reusch, Norbert Jesse (Hrsg.): Informatik bewegt – Informatik 2002 – 32. Jahrestagung der Gesellschaft für Informatik e.V. (GI) 30.Sept.-3.Okt. 2002 in Dortmund (Ergänzungsband).

P-21 Jörg Desel, Mathias Weske (Hrsg.): Promise 2002: Prozessorientierte Methoden und Werkzeuge für die Entwicklung von Informationssystemen.

P-22 Sigrid Schubert, Johannes Magenheim, Peter Hubwieser, Torsten Brinda (Hrsg.): Forschungsbeiträge zur "Didaktik der Informatik" – Theorie, Praxis, Evaluation.

P-23 Thorsten Spitta, Jens Borchers, Harry M. Sneed (Hrsg.): Software Management 2002 – Fortschritt durch Beständigkeit

P-24 Rainer Eckstein, Robert Tolksdorf (Hrsg.): XMIDX 2003 – XML-Technologien für Middleware – Middleware für XML-Anwendungen

P-25 Key Pousttchi, Klaus Turowski (Hrsg.): Mobile Commerce – Anwendungen und Perspektiven – 3. Workshop Mobile Commerce, Universität Augsburg, 04.02.2003

P-26 Gerhard Weikum, Harald Schöning, Erhard Rahm (Hrsg.): BTW 2003: Datenbanksysteme für Business, Technologie und Web

P-27 Michael Kroll, Hans-Gerd Lipinski, Kay Melzer (Hrsg.): Mobiles Computing in der Medizin

P-28 Ulrich Reimer, Andreas Abecker, Steffen Staab, Gerd Stumme (Hrsg.): WM 2003: Professionelles Wissensmanagement – Erfahrungen und Visionen

P-29 Antje Düsterhöft, Bernhard Thalheim (Eds.): NLDB'2003: Natural Language Processing and Information Systems

P-30 Mikhail Godlevsky, Stephen Liddle, Heinrich C. Mayr (Eds.): Information Systems Technology and its Applications

P-31 Arslan Brömme, Christoph Busch (Eds.): BIOSIG 2003: Biometrics and Electronic Signatures

P-32 Peter Hubwieser (Hrsg.): Informatische Fachkonzepte im Unterricht – INFOS 2003

P-33 Andreas Geyer-Schulz, Alfred Taudes (Hrsg.): Informationswirtschaft: Ein Sektor mit Zukunft

P-34 Klaus Dittrich, Wolfgang König, Andreas Oberweis, Kai Rannenberg, Wolfgang Wahlster (Hrsg.): Informatik 2003 – Innovative Informatikanwendungen (Band 1)

P-35 Klaus Dittrich, Wolfgang König, Andreas Oberweis, Kai Rannenberg, Wolfgang Wahlster (Hrsg.): Informatik 2003 – Innovative Informatikanwendungen (Band 2)

P-36 Rüdiger Grimm, Hubert B. Keller, Kai Rannenberg (Hrsg.): Informatik 2003 – Mit Sicherheit Informatik

P-37 Arndt Bode, Jörg Desel, Sabine Rathmayer, Martin Wessner (Hrsg.): DeLFI 2003: e-Learning Fachtagung Informatik

P-38 E.J. Sinz, M. Plaha, P. Neckel (Hrsg.): Modellierung betrieblicher Informationssysteme – MobIS 2003

P-39 Jens Nedon, Sandra Frings, Oliver Göbel (Hrsg.): IT-Incident Management & IT-Forensics – IMF 2003

P-40 Michael Rebstock (Hrsg.): Modellierung betrieblicher Informationssysteme – MobIS 2004

P-41 Uwe Brinkschulte, Jürgen Becker, Dietmar Fey, Karl-Erwin Großpietsch, Christian Hochberger, Erik Maehle, Thomas Runkler (Edts.): ARCS 2004 – Organic and Pervasive Computing

P-42 Key Pousttchi, Klaus Turowski (Hrsg.): Mobile Economy – Transaktionen und Prozesse, Anwendungen und Dienste

P-43 Birgitta König-Ries, Michael Klein, Philipp Obreiter (Hrsg.): Persistance, Scalability, Transactions – Database Mechanisms for Mobile Applications

P-44 Jan von Knop, Wilhelm Haverkamp, Eike Jessen (Hrsg.): Security, E-Learning. E-Services

P-45 Bernhard Rumpe, Wofgang Hesse (Hrsg.): Modellierung 2004

P-46 Ulrich Flegel, Michael Meier (Hrsg.): Detection of Intrusions of Malware & Vulnerability Assessment

P-47 Alexander Prosser, Robert Krimmer (Hrsg.): Electronic Voting in Europe – Technology, Law, Politics and Society

P-48 Anatoly Doroshenko, Terry Halpin, Stephen W. Liddle, Heinrich C. Mayr (Hrsg.): Information Systems Technology and its Applications

P-49 G. Schiefer, P. Wagner, M. Morgenstern, U. Rickert (Hrsg.): Integration und Datensicherheit – Anforderungen, Konflikte und Perspektiven

P-50 Peter Dadam, Manfred Reichert (Hrsg.): INFORMATIK 2004 – Informatik verbindet (Band 1) Beiträge der 34. Jahrestagung der Gesellschaft für Informatik e.V. (GI), 20.-24. September 2004 in Ulm

P-51 Peter Dadam, Manfred Reichert (Hrsg.): INFORMATIK 2004 – Informatik verbindet (Band 2) Beiträge der 34. Jahrestagung der Gesellschaft für Informatik e.V. (GI), 20.-24. September 2004 in Ulm

P-52 Gregor Engels, Silke Seehusen (Hrsg.): DELFI 2004 – Tagungsband der 2. e-Learning Fachtagung Informatik

P-53 Robert Giegerich, Jens Stoye (Hrsg.): German Conference on Bioinformatics – GCB 2004

P-54 Jens Borchers, Ralf Kneuper (Hrsg.): Softwaremanagement 2004 – Outsourcing und Integration

P-55 Jan von Knop, Wilhelm Haverkamp, Eike Jessen (Hrsg.): E-Science und Grid Adhoc-Netze Medienintegration

P-56 Fernand Feltz, Andreas Oberweis, Benoit Otjacques (Hrsg.): EMISA 2004 – Informationssysteme im E-Business und E-Government

P-57 Klaus Turowski (Hrsg.): Architekturen, Komponenten, Anwendungen

P-58 Sami Beydeda, Volker Gruhn, Johannes Mayer, Ralf Reussner, Franz Schweiggert (Hrsg.): Testing of Component-Based Systems and Software Quality

P-59 J. Felix Hampe, Franz Lehner, Key Pousttchi, Kai Ranneberg, Klaus Turowski (Hrsg.): Mobile Business – Processes, Platforms, Payments

P-60 Steffen Friedrich (Hrsg.): Unterrichtskonzepte für inforrmatische Bildung

P-61 Paul Müller, Reinhard Gotzhein, Jens B. Schmitt (Hrsg.): Kommunikation in verteilten Systemen

P-62 Federrath, Hannes (Hrsg.): „Sicherheit 2005“ – Sicherheit – Schutz und Zuverlässigkeit

P-63 Roland Kaschek, Heinrich C. Mayr, Stephen Liddle (Hrsg.): Information Systems – Technology and ist Applications

P-64 Peter Liggesmeyer, Klaus Pohl, Michael Goedicke (Hrsg.): Software Engineering 2005

P-65 Gottfried Vossen, Frank Leymann, Peter Lockemann, Wolffried Stucky (Hrsg.): Datenbanksysteme in Business, Technologie und Web

P-66 Jörg M. Haake, Ulrike Lucke, Djamshid Tavangarian (Hrsg.): DeLFI 2005: 3. deutsche e-Learning Fachtagung Informatik

P-67 Armin B. Cremers, Rainer Manthey, Peter Martini, Volker Steinhage (Hrsg.): INFORMATIK 2005 – Informatik LIVE (Band 1)

P-68 Armin B. Cremers, Rainer Manthey, Peter Martini, Volker Steinhage (Hrsg.): INFORMATIK 2005 – Informatik LIVE (Band 2)

P-69 Robert Hirschfeld, Ryszard Kowalcyk, Andreas Polze, Matthias Weske (Hrsg.): NODe 2005, GSEM 2005

P-70 Klaus Turowski, Johannes-Maria Zaha (Hrsg.): Component-oriented Enterprise Application (COAE 2005)

P-71 Andrew Torda, Stefan Kurz, Matthias Rarey (Hrsg.): German Conference on Bioinformatics 2005

P-72 Klaus P. Jantke, Klaus-Peter Fähnrich, Wolfgang S. Wittig (Hrsg.): Marktplatz Internet: Von e-Learning bis e-Payment

P-73 Jan von Knop, Wilhelm Haverkamp, Eike Jessen (Hrsg.): “Heute schon das Morgen sehen“

P-74 Christopher Wolf, Stefan Lucks, Po-Wah Yau (Hrsg.): WEWoRC 2005 – Western European Workshop on Research in Cryptology

P-75 Jörg Desel, Ulrich Frank (Hrsg.): Enterprise Modelling and Information Systems Architecture

P-76 Thomas Kirste, Birgitta König-Riess, Key Pousttchi, Klaus Turowski (Hrsg.): Mobile Informationssysteme – Potentiale, Hindernisse, Einsatz

P-77 Jana Dittmann (Hrsg.): SICHERHEIT 2006

P-78 K.-O. Wenkel, P. Wagner, M. Morgenstern, K. Luzi, P. Eisermann (Hrsg.): Land- und Ernährungswirtschaft im Wandel

P-79 Bettina Biel, Matthias Book, Volker Gruhn (Hrsg.): Softwareengineering 2006

P-80 Mareike Schoop, Christian Huemer, Michael Rebstock, Martin Bichler (Hrsg.): Service-Oriented Electronic Commerce

P-81 Wolfgang Karl, Jürgen Becker, Karl-Erwin Großpietsch, Christian Hochberger, Erik Maehle (Hrsg.): ARCS´06

P-82 Heinrich C. Mayr, Ruth Breu (Hrsg.): Modellierung 2006

P-83 Daniel Huson, Oliver Kohlbacher, Andrei Lupas, Kay Nieselt and Andreas Zell (eds.): German Conference on Bioinformatics

P-84 Dimitris Karagiannis, Heinrich C. Mayr, (Hrsg.): Information Systems Technology and its Applications

P-85 Witold Abramowicz, Heinrich C. Mayr, (Hrsg.): Business Information Systems

P-86 Robert Krimmer (Ed.): Electronic Voting 2006

P-87 Max Mühlhäuser, Guido Rößling, Ralf Steinmetz (Hrsg.): DELFI 2006: 4. e-Learning Fachtagung Informatik

P-88 Robert Hirschfeld, Andreas Polze, Ryszard Kowalczyk (Hrsg.): NODe 2006, GSEM 2006

P-90 Joachim Schelp, Robert Winter, Ulrich Frank, Bodo Rieger, Klaus Turowski (Hrsg.): Integration, Informationslogistik und Architektur

P-91 Henrik Stormer, Andreas Meier, Michael Schumacher (Eds.): European Conference on eHealth 2006

P-92 Fernand Feltz, Benoît Otjacques, Andreas Oberweis, Nicolas Poussing (Eds.): AIM 2006

P-93 Christian Hochberger, Rüdiger Liskowsky (Eds.): INFORMATIK 2006 – Informatik für Menschen, Band 1

P-94 Christian Hochberger, Rüdiger Liskowsky (Eds.): INFORMATIK 2006 – Informatik für Menschen, Band 2

P-95 Matthias Weske, Markus Nüttgens (Eds.): EMISA 2005: Methoden, Konzepte und Technologien für die Entwicklung von dienstbasierten Informationssystemen

P-96 Saartje Brockmans, Jürgen Jung, York Sure (Eds.): Meta-Modelling and Ontologies

P-97 Oliver Göbel, Dirk Schadt, Sandra Frings, Hardo Hase, Detlef Günther, Jens Nedon (Eds.): IT-Incident Mangament & IT-Forensics – IMF 2006

P-98 Hans Brandt-Pook, Werner Simonsmeier und Thorsten Spitta (Hrsg.): Beratung in der Softwareentwicklung – Modelle, Methoden, Best Practices

P-99 Andreas Schwill, Carsten Schulte, Marco Thomas (Hrsg.): Didaktik der Informatik

P-100 Peter Forbrig, Günter Siegel, Markus Schneider (Hrsg.): HDI 2006: Hochschuldidaktik der Informatik

P-101 Stefan Böttinger, Ludwig Theuvsen, Susanne Rank, Marlies Morgenstern (Hrsg.): Agrarinformatik im Spannungsfeld zwischen Regionalisierung und globalen Wertschöpfungsketten

P-102 Otto Spaniol (Eds.): Mobile Services and Personalized Environments

P-103 Alfons Kemper, Harald Schöning, Thomas Rose, Matthias Jarke, Thomas Seidl, Christoph Quix, Christoph Brochhaus (Hrsg.): Datenbanksysteme in Business, Technologie und Web (BTW 2007)

P-104 Birgitta König-Ries, Franz Lehner, Rainer Malaka, Can Türker (Hrsg.) MMS 2007: Mobilität und mobile Informationssysteme

P-105 Wolf-Gideon Bleek, Jörg Raasch, Heinz Züllighoven (Hrsg.) Software Engineering 2007

P-106 Wolf-Gideon Bleek, Henning Schwentner, Heinz Züllighoven (Hrsg.) Software Engineering 2007 – Beiträge zu den Workshops

P-107 Heinrich C. Mayr, Dimitris Karagiannis (eds.) Information Systems Technology and its Applications

P-108 Arslan Brömme, Christoph Busch, Detlef Hühnlein (eds.) BIOSIG 2007: Biometrics and Electronic Signatures

P-109 Rainer Koschke, Otthein Herzog, Karl-Heinz Rödiger, Marc Ronthaler (Hrsg.) INFORMATIK 2007 Informatik trifft Logistik Band 1

P-110 Rainer Koschke, Otthein Herzog, Karl-Heinz Rödiger, Marc Ronthaler (Hrsg.) INFORMATIK 2007 Informatik trifft Logistik Band 2

P-111 Christian Eibl, Johannes Magenheim, Sigrid Schubert, Martin Wessner (Hrsg.) DeLFI 2007: 5. e-Learning Fachtagung Informatik

P-112 Sigrid Schubert (Hrsg.) Didaktik der Informatik in Theorie und Praxis

P-113 Sören Auer, Christian Bizer, Claudia Müller, Anna V. Zhdanova (Eds.) The Social Semantic Web 2007 Proceedings of the 1st Conference on Social Semantic Web (CSSW)

P-114 Sandra Frings, Oliver Göbel, Detlef Günther, Hardo G. Hase, Jens Nedon, Dirk Schadt, Arslan Brömme (Eds.) IMF2007 IT-incident management & IT-forensics Proceedings of the 3rd International Conference on IT-Incident Management & IT-Forensics

P-115 Claudia Falter, Alexander Schliep, Joachim Selbig, Martin Vingron and Dirk Walther (Eds.) German conference on bioinformatics GCB 2007

P-116 Witold Abramowicz, Leszek Maciszek (Eds.) Business Process and Services Computing 1st International Working Conference on Business Process and Services Computing BPSC 2007

P-117 Ryszard Kowalczyk (Ed.) Grid service engineering and manegement The 4th International Conference on Grid Service Engineering and Management GSEM 2007

P-118 Andreas Hein, Wilfried Thoben, Hans-Jürgen Appelrath, Peter Jensch (Eds.) European Conference on ehealth 2007

P-119 Manfred Reichert, Stefan Strecker, Klaus Turowski (Eds.) Enterprise Modelling and Information Systems Architectures Concepts and Applications

P-120 Adam Pawlak, Kurt Sandkuhl, Wojciech Cholewa, Leandro Soares Indrusiak (Eds.) Coordination of Collaborative Engineering - State of the Art and Future Challenges

P-121 Korbinian Herrmann, Bernd Bruegge (Hrsg.) Software Engineering 2008 Fachtagung des GI-Fachbereichs Softwaretechnik

P-122 Walid Maalej, Bernd Bruegge (Hrsg.) Software Engineering 2008 - Workshopband Fachtagung des GI-Fachbereichs Softwaretechnik

P-123 Michael H. Breitner, Martin Breunig, Elgar Fleisch, Ley Pousttchi, Klaus Turowski (Hrsg.)
Mobile und Ubiquitäre Informationssysteme – Technologien, Prozesse, Marktfähigkeit
Proceedings zur 3. Konferenz Mobile und Ubiquitäre Informationssysteme (MMS 2008)

P-124 Wolfgang E. Nagel, Rolf Hoffmann, Andreas Koch (Eds.)
9th Workshop on Parallel Systems and Algorithms (PASA)
Workshop of the GI/ITG Speciel Interest Groups PARS and PARVA

P-125 Rolf A.E. Müller, Hans-H. Sundermeier, Ludwig Theuvsen, Stephanie Schütze, Marlies Morgenstern (Hrsg.)
Unternehmens-IT: Führungsinstrument oder Verwaltungsbürde
Referate der 28. GIL Jahrestagung

P-126 Rainer Gimnich, Uwe Kaiser, Jochen Quante, Andreas Winter (Hrsg.)
10th Workshop Software Reengineering (WSR 2008)

P-127 Thomas Kühne, Wolfgang Reisig, Friedrich Steimann (Hrsg.)
Modellierung 2008

P-128 Ammar Alkassar, Jörg Siekmann (Hrsg.)
Sicherheit 2008
Sicherheit, Schutz und Zuverlässigkeit
Beiträge der 4. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI)
2.-4. April 2008
Saarbrücken, Germany

P-129 Wolfgang Hesse, Andreas Oberweis (Eds.)
Sigsand-Europe 2008
Proceedings of the Third AIS SIGSAND European Symposium on Analysis, Design, Use and Societal Impact of Information Systems

P-130 Paul Müller, Bernhard Neumair, Gabi Dreo Rodosek (Hrsg.)
1. DFN-Forum Kommunikations-technologien Beiträge der Fachtagung

P-131 Robert Krimmer, Rüdiger Grimm (Eds.)
3rd International Conference on Electronic Voting 2008
Co-organized by Council of Europe, Gesellschaft für Informatik and E-Voting.CC

P-132 Silke Seehusen, Ulrike Lucke, Stefan Fischer (Hrsg.)
DeLFI 2008:
Die 6. e-Learning Fachtagung Informatik

P-133 Heinz-Gerd Hegering, Axel Lehmann, Hans Jürgen Ohlbach, Christian Scheideler (Hrsg.)
INFORMATIK 2008
Beherrschbare Systeme – dank Informatik
Band 1

P-134 Heinz-Gerd Hegering, Axel Lehmann, Hans Jürgen Ohlbach, Christian Scheideler (Hrsg.)
INFORMATIK 2008
Beherrschbare Systeme – dank Informatik
Band 2

P-135 Torsten Brinda, Michael Fothe, Peter Hubwieser, Kirsten Schlüter (Hrsg.)
Didaktik der Informatik – Aktuelle Forschungsergebnisse

P-136 Andreas Beyer, Michael Schroeder (Eds.)
German Conference on Bioinformatics GCB 2008

P-137 Arslan Brömme, Christoph Busch, Detlef Hühnlein (Eds.)
BIOSIG 2008: Biometrics and Electronic Signatures

P-138 Barbara Dinter, Robert Winter, Peter Chamoni, Norbert Gronau, Klaus Turowski (Hrsg.)
Synergien durch Integration und Informationslogistik
Proceedings zur DW2008

P-139 Georg Herzwurm, Martin Mikusz (Hrsg.)
Industrialisierung des Software-Managements
Fachtagung des GI-Fachausschusses Management der Anwendungsentwick-lung und -wartung im Fachbereich Wirtschaftsinformatik

P-140 Oliver Göbel, Sandra Frings, Detlef Günther, Jens Nedon, Dirk Schadt (Eds.)
IMF 2008 - IT Incident Management & IT Forensics

P-141 Peter Loos, Markus Nüttgens, Klaus Turowski, Dirk Werth (Hrsg.)
Modellierung betrieblicher Informations-systeme (MobIS 2008)
Modellierung zwischen SOA und Compliance Management

P-142 R. Bill, P. Korduan, L. Theuvsen, M. Morgenstern (Hrsg.)
Anforderungen an die Agrarinformatik durch Globalisierung und Klimaveränderung

P-143 Peter Liggesmeyer, Gregor Engels, Jürgen Münch, Jörg Dörr, Norman Riegel (Hrsg.)
Software Engineering 2009
Fachtagung des GI-Fachbereichs Softwaretechnik

P-144 Johann-Christoph Freytag, Thomas Ruf, Wolfgang Lehner, Gottfried Vossen (Hrsg.)
Datenbanksysteme in Business, Technologie und Web (BTW)

P-145 Knut Hinkelmann, Holger Wache (Eds.)
WM2009: 5th Conference on Professional Knowledge Management

P-146 Markus Bick, Martin Breunig, Hagen Höpfner (Hrsg.)
Mobile und Ubiquitäre Informationssysteme – Entwicklung, Implementierung und Anwendung
4. Konferenz Mobile und Ubiquitäre Informationssysteme (MMS 2009)

P-147 Witold Abramowicz, Leszek Maciaszek, Ryszard Kowalczyk, Andreas Speck (Eds.)
Business Process, Services Computing and Intelligent Service Management
BPSC 2009 · ISM 2009 · YRW-MBP 2009

P-148 Christian Erfurth, Gerald Eichler, Volkmar Schau (Eds.)
9th International Conference on Innovative Internet Community Systems
I²CS 2009

P-149 Paul Müller, Bernhard Neumair, Gabi Dreo Rodosek (Hrsg.)
2. DFN-Forum Kommunikationstechnologien
Beiträge der Fachtagung

P-150 Jürgen Münch, Peter Liggesmeyer (Hrsg.)
Software Engineering
2009 - Workshopband

P-151 Armin Heinzl, Peter Dadam, Stefan Kirn, Peter Lockemann (Eds.)
PRIMIUM
Process Innovation for Enterprise Software

P-152 Jan Mendling, Stefanie Rinderle-Ma, Werner Esswein (Eds.)
Enterprise Modelling and Information Systems Architectures
Proceedings of the 3rd Int'l Workshop EMISA 2009

P-153 Andreas Schwill, Nicolas Apostolopoulos (Hrsg.)
Lernen im Digitalen Zeitalter
DeLFI 2009 – Die 7. E-Learning Fachtagung Informatik

P-154 Stefan Fischer, Erik Maehle Rüdiger Reischuk (Hrsg.)
INFORMATIK 2009
Im Focus das Leben

P-155 Arslan Brömme, Christoph Busch, Detlef Hühnlein (Eds.)
BIOSIG 2009:
Biometrics and Electronic Signatures
Proceedings of the Special Interest Group on Biometrics and Electronic Signatures

P-156 Bernhard Koerber (Hrsg.)
Zukunft braucht Herkunft
25 Jahre »INFOS – Informatik und Schule«

P-157 Ivo Grosse, Steffen Neumann, Stefan Posch, Falk Schreiber, Peter Stadler (Eds.)
German Conference on Bioinformatics 2009

P-158 W. Claupein, L. Theuvsen, A. Kämpf, M. Morgenstern (Hrsg.)
Precision Agriculture Reloaded – Informationsgestützte Landwirtschaft

P-159 Gregor Engels, Markus Luckey, Wilhelm Schäfer (Hrsg.)
Software Engineering 2010

P-160 Gregor Engels, Markus Luckey, Alexander Pretschner, Ralf Reussner (Hrsg.)
Software Engineering 2010 – Workshopband
(inkl. Doktorandensymposium)

P-161 Gregor Engels, Dimitris Karagiannis Heinrich C. Mayr (Hrsg.)
Modellierung 2010

P-162 Maria A. Wimmer, Uwe Brinkhoff, Siegfried Kaiser, Dagmar Lück-Schneider, Erich Schweighofer, Andreas Wiebe (Hrsg.)
Vernetzte IT für einen effektiven Staat
Gemeinsame Fachtagung Verwaltungsinformatik (FTVI) und Fachtagung Rechtsinformatik (FTRI) 2010

P-163 Markus Bick, Stefan Eulgem, Elgar Fleisch, J. Felix Hampe, Birgitta König-Ries, Franz Lehner, Key Pousttchi, Kai Rannenberg (Hrsg.)
Mobile und Ubiquitäre Informationssysteme
Technologien, Anwendungen und Dienste zur Unterstützung von mobiler Kollaboration

P-166 Paul Müller, Bernhard Neumair, Gabi Dreo Rodosek (Hrsg.)
3. DFN-Forum Kommunikationstechnologien
Beiträge der Fachtagung

The titles can be purchased at:

Köllen Druck + Verlag GmbH
Ernst-Robert-Curtius-Str. 14 · D-53117 Bonn
Fax: +49 (0)228/9898222
E-Mail: druckverlag@koellen.de