GWDG-Bericht Nr. 70

Christoph Gartmann, Jochen Jähnke
(Hrsg.)

22. DV-Treffen der Max-Planck-Institute

**16. - 18. November 2005
in Göttingen**

Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

Christoph Gartmann, Jochen Jähnke (Hrsg.)

22. DV-Treffen der Max-Planck-Institute

16. - 18. November 2005
in Göttingen

Christoph Gartmann, Jochen Jähnke (Hrsg.)

22. DV-Treffen der Max-Planck-Institute

16. - 18. November 2005
in Göttingen

GWDG-Bericht Nr. 70
Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen
Am Faßberg
D-37077 Göttingen
Telefon: 0551 201-1510
Telefax: 0551 201-2150
E-Mail: gwdg@gwdg.de

Satz: Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

Druck: Artificium Stietenroth, Bodenfelde

ISSN 0176-2516

Inhalt

Vorwort

Der vorliegende Band enthält mehrere Beiträge des 22. DV-Treffens der Max-Planck-Institute, das vom 16. bis 18. November 2005 bei der GWDG in Göttingen stattfand.

Eine vollständigere, elektronische Zusammenstellung der Vorträge befindet sich im IT-Portal der MPG (https://it-portal.mpg.de) unter „DV-Treffen der Institute“.

Das Treffen begann wieder mit mehreren parallelen Workshops zu ausgesuchten Problemstellungen aus dem Tätigkeitsbereich der EDV-Abteilungen. Danach schlossen sich zwei Tage mit Vorträgen an. Die Hauptthemen des Treffens waren Grid-Computing, Content- und Dokumenten-Management-Systeme, Computersicherheit sowie die rechtlichen Aspekte der Administration von Rechnern und Netzen. Auch die Themen IP-Telefonie, Virtualisierung und Langzeitarchivierung wurden behandelt.

Den inzwischen schon fast traditionellen „Blick über den Tellerrand“ ermöglichten zwei Vorträge anderer Forschungsgesellschaften. Eine Mitarbeiterin der Fraunhofer Gesellschaft berichtete über die IT-Weiterbildung in der FHG und ein weiterer - hier vertretener - Vortrag gab einen Einblick in die IT-Landschaft der Helmholtz-Gemeinschaft deutscher Forschungszentren.

Die Veranstaltung dient hauptsächlich dem Austausch zwischen den EDV-Abteilungen der einzelnen Institute und gibt regelmäßig wichtige Hilfen und

Impulse auch für die praktische, tägliche Arbeit. Als ein Treffen, das von den Beteiligten jeweils selbst organisiert wird, kann diese Veranstaltung immer aktuell auf die wichtigen Themen und Wünsche eingehen und sich den laufenden Veränderungen anpassen. Als scheidende Veranstalter hoffen wir, dass es uns gelungen ist, das hohe Niveau zu halten und möchten es nicht versäumen, uns bei der GWDG für die Organisation vor Ort herzlich zu bedanken, insbesondere bei Herrn Otto, der wieder die Hauptlast in Göttingen trug.

Freiburg, 10.10.2006 Christoph Gartmann, Jochen Jähnke

VMware 5.x: not undoable – neue Konzepte für die virtuellen Festplatten

Ulrich Schwardmann

Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

Die Firma VMware hat mit der Version 5.x eine umfangreiche Überarbeitung der bisherigen Konzepte in VMware vorgenommen. Dies betrifft sowohl die Oberfläche als auch die zugrundeliegenden Prinzipien der Organisation der virtuellen Festplatten. Einige alte liebgewonnene Vorgehensweisen sind in allgemeinere Konzepte übergegangen, treten zum Teil stark in den Hintergrund und sind in einigen Fällen sogar vollständig abgelöst worden.

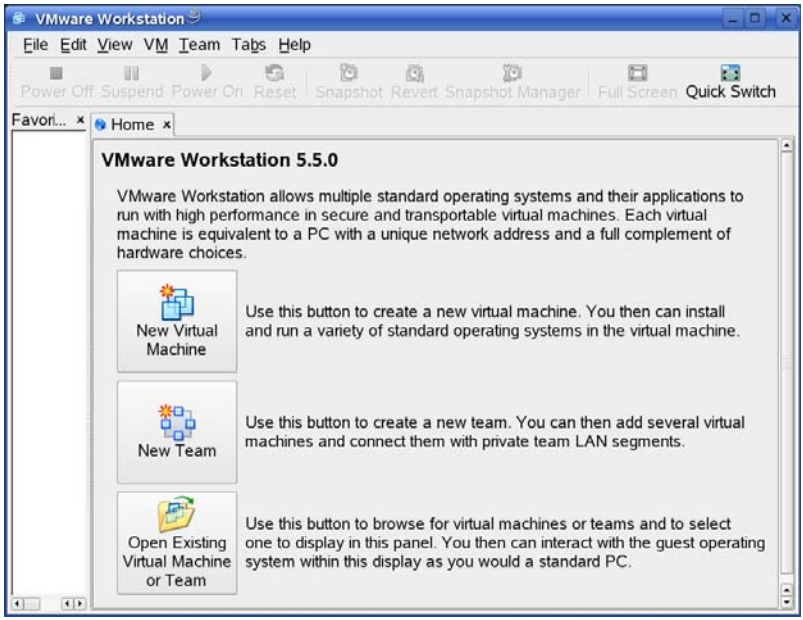


Abb. 1: Die VM-Konsole als Hilfe zur Einrichtung von VMs ...

1. Look & Feel

Das VMware-Fenster ist mit der 5er Version zu einer Zentrale zur Erzeugung und Steuerung von einzelnen und Gruppen von VMware-Maschinen umgebaut worden. Beim Start wird ein Dialog eröffnet, bei dem bestehende Virtuelle Maschinen (VMs) hochgefahren werden können, oder neue VMs oder ganze Teams von VMs erzeugt werden können. Dieses Fenster bleibt auch weiterhin über den Reiter „Home“ während der Laufzeit von VMware erreichbar.

Nachdem VMs auf die eine oder andere Art zur Verfügung gestellt wurden, sind diese als weitere Reiter im Fenster erreichbar. Sie befinden sich zunächst im nicht gestarteten Zustand und können mit den entsprechenden Schaltflächen noch in ihren Eigenschaften gestaltet werden bzw. gestartet werden. Eine weitere Möglichkeit besteht bereits hier darin, einen Klon der vorliegenden Maschine zu erzeugen, doch dazu weiter unten.

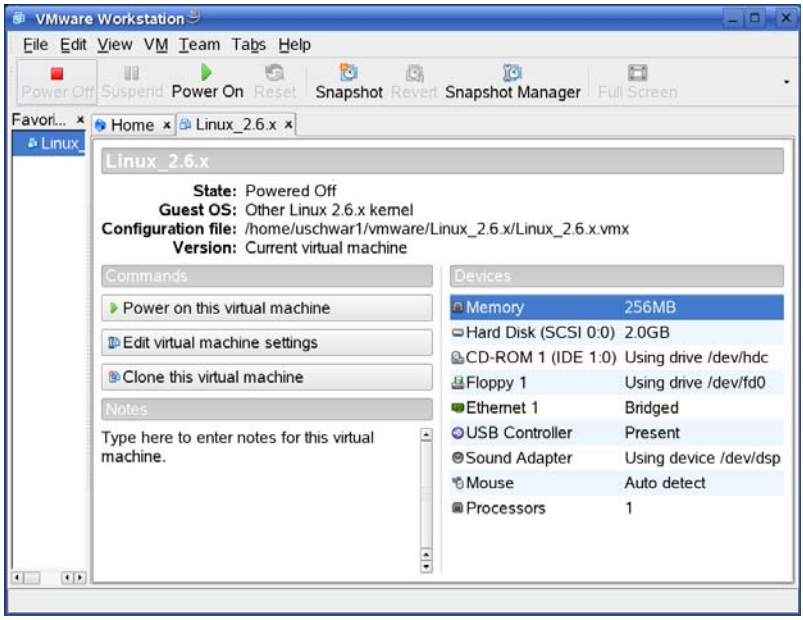


Abb. 2: ... und als Hilfe zur Konfiguration und Steuerung von VMs

2. Die alten und neuen Konzepte von VMware 5.x

Bereits mit dem Aufbau dieser Eingangs-Fenster von VMware 5.x wird deutlich, dass sich einige wesentliche konzeptionelle Neuerungen in dieser Version befinden. Doch zunächst noch eine kurze Beschreibung der wichtigsten Konzepte für die Nutzung von Festplatten, so wie sie in den vorangegangenen Versionen bekannt gewesen sind:

- **persistent:** Bei dieser Betriebsart werden alle Änderungen, die während der Laufzeit einer VM auf der Platte vorgenommen werden, dauerhaft in die virtuelle Platte aufgenommen. Dies entspricht dem Verhalten, wie es ja auch von einer realen Maschine erwartet wird.
- **nonpersistent:** Hier werden alle Änderungen, die während der Laufzeit einer VM auf der Platte vorgenommen werden, nach dem Ausschalten der VM wieder verworfen. Dies ist eine Möglichkeit, die aus der Sicht einer realen Maschine zunächst gewöhnungsbedürftig ist, die aber für verschiedene Zwecke enorme Vorteile bietet. Seine Berechtigung bekommt dieses Konzept insbesondere dadurch, dass eine Entscheidung

für den Plattenmodus immer neu getroffen werden kann, wenn sich die Maschine im ausgeschalteten Zustand befindet.

- **undoable:** Bei diesem Platten-Modus sind alle Änderungen revidierbar in dem Sinne, dass nach dem Stop der VM der Benutzer entscheiden kann, ob die Änderungen eingepflegt werden sollen oder nicht, oder auch, ob diese Entscheidung auf später vertagt werden soll.

Grundsätzlich beruhen diese Modi darauf, dass durch die Virtualisierung der Platten eine Zwischenschicht zwischen realer Hardware und VM eingezogen wurde. Diese besteht darin, eine virtuelle Platte als eine Datei bzw. Gruppe von Dateien zu beschreiben. Der Plattencache lässt sich dann ebenfalls als eine solche Datei beschreiben, der dadurch zudem den Vorteil hat, beliebig wachsen zu können. Die Entscheidung zwischen den drei bisherigen Plattenmodi ist auf dieser Ebene schlicht die Entscheidung, ob der Plattencache immer in die virtuelle Platte eingepflegt wird, nie eingepflegt wird, oder ob der Plattencache für später aufgehoben wird.

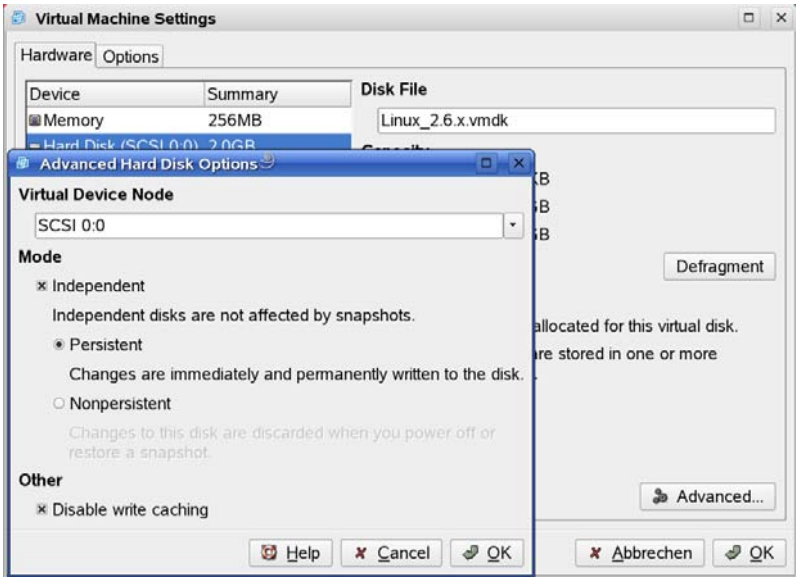


Abb. 3: Die Einstellung „independent“ findet sich unter den Plattenseigenschaften in der Rubrik „erweitert“.

Was wurde nun aus diesen drei Konzepten mit der neuen VMware-Version?

Die gute Nachricht ist, dass zumindest persistent und nonpersistent in dieser Version noch verfügbar sind. Aber die schlechte Nachricht ist eben, dass für

diese Konzepte ein neuer Plattenmodus geschaffen wurde, der nicht der normale Modus ist und der in der Konfiguration schwer zu finden ist. Damit erfüllt dieser Modus wichtige Eigenschaften, die darauf hindeuten, dass er bei nächster Gelegenheit abgelöst zu werden droht.

Dieser neue Modus wird als independent oder unabhängig bezeichnet und ist über die erweiterten Eigenschaften der Plattenkonfiguration zu erreichen. Insbesondere sind unter diesem Plattenmodus neuere Konzepte, wie Snapshots, nicht erlaubt.

Gerade diese Snapshots sind es nun, die den Ersatz für das bisherige Konzept 'undoable' bilden.

3. Snapshots

Die Zustände einer „undoable disk“ waren gewissermaßen Momentaufnahmen einer VM zu bestimmten Zeitpunkten, nämlich vor und nach der letzten Laufperiode einer virtuellen Maschine. Genau nach dieser Sichtweise arbeiten nun die so genannten Snapshots, nur mit der zusätzlichen Eigenschaft, dass derartige Momentaufnahmen jederzeit gemacht und gespeichert werden können. Auch die zugrundeliegende Technik beruht gleichermassen auf der Verwendung von Plattencaches. Nur was bislang als eine Platte und ein Platencache organisiert war, kann nunmehr ein ganzes System solcher Plattencaches werden.

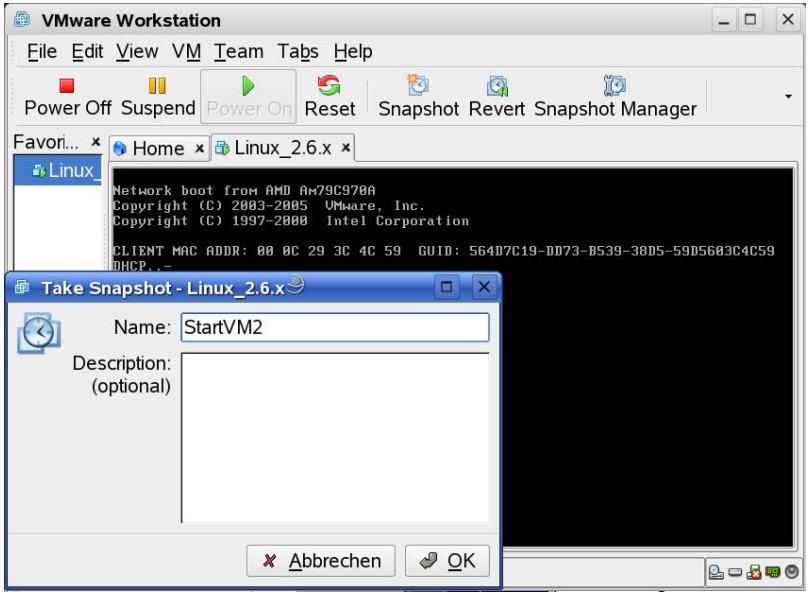


Abb. 4: Der Snapshot-Dialog

Um eine solche Struktur noch im Griff zu behalten, ist in den VMware-Desktop ein eigener Snapshot-Manager eingebaut worden, der die beliebig komplizierte Situation durch eine grafische Darstellung des Snapshot-Baumes handhabbar zu machen versucht.

Wer aber versucht sein sollte, alte Techniken, wie das Kopieren von virtuellen Festplatten an andere Orte von Hand, zu verwenden, dem wird schnell die neue Komplexität auf Dateiebene zum Graus werden. Die Vorteile der einfachen Struktur früherer Versionen sind hier leider völlig verloren gegangen.

Grundsätzlich ließen sich solche Snapshots, wie es denn auch von VMware besonders angepriesen wird, in idealer Weise zur Gestaltung von Kursen einsetzen. Jeder Snapshot könnte ein definierter Punkt sein, den alle Kursteilnehmer jeweils als neuen Ausgangspunkt eines inhaltlichen Abschnitts verwenden.

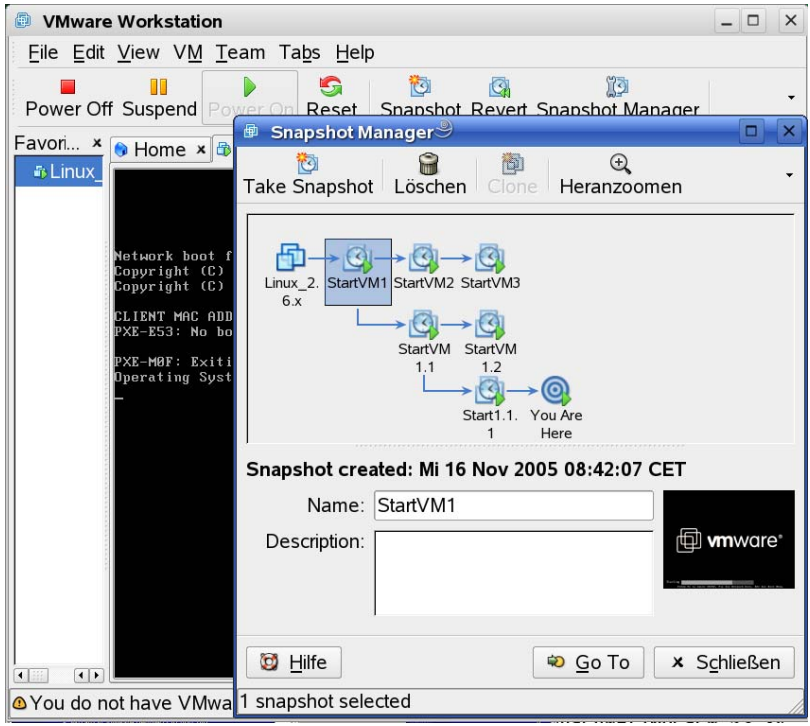


Abb. 5: Snapshot-Manager: verzweigte Bäume sind möglich

Leider steht einer derartigen Vorgehensweise die Betriebssystem-Lizenzvergabe eines gewissen Software-Unternehmens entgegen, das für jede Instanz einer Maschine, real oder virtuell, die Erzeugung einer eigenen System-ID vorsieht. Dies müsste nun nicht nur für jeden Klon, sondern auch für jeden geklonten Snapshot geschehen – ein nicht mehr zu rechtfertigender Aufwand.

Für die Abhaltung von Kursen, die keine derartig restriktive Lizenzpolitik voraussetzen, kann sich das Snapshot-Konzept aber noch als ein sehr wirkungsvolles didaktisches Instrument erweisen.

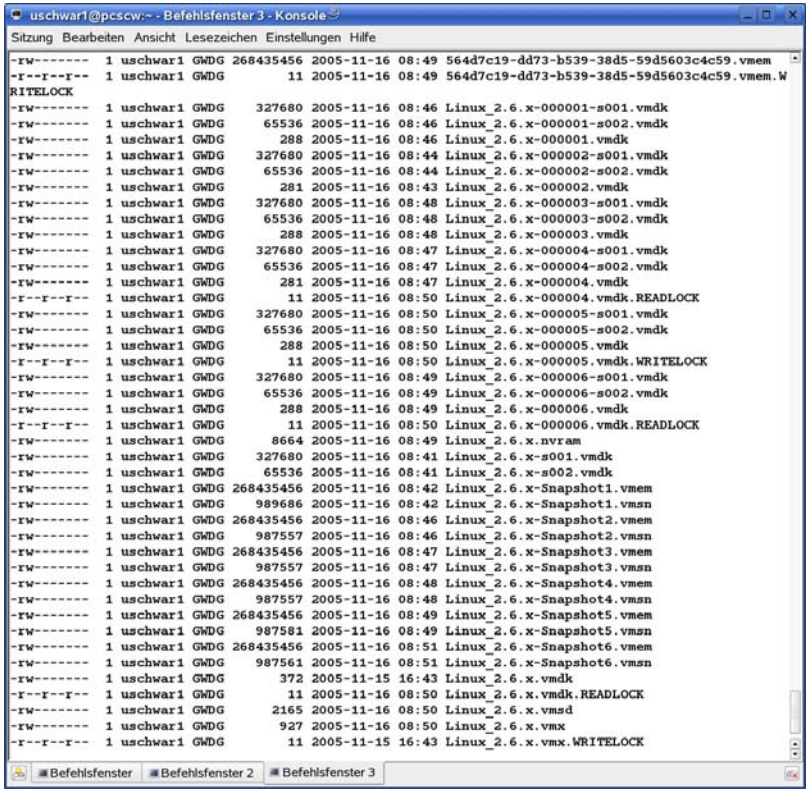


Abb. 6: Die Dateistruktur selbst wird durch das Anlegen von Snapshots wesentlich komplexer

4. Klone – die Kopien einer VM

Eine Möglichkeit, die erfahrenen VMware-Nutzern natürlich sehr geläufig ist, ist das Erzeugen der Kopie einer bestehenden Maschine. Was bislang allerdings im wesentlichen von Hand durch die Kopie der virtuellen Platten erzeugt wurde, bekommt nun eine eigene Nutzerschnittstelle.

Zudem werden aber auch hier wieder die Möglichkeiten eingeführt, die sich durch das Daten-Caching gegenüber den virtuellen Platten ergeben. Neben der „vollständigen“ Kopie einer Platte, so wie es auch von Hand durch die Kopie der Platte gemacht wird, gibt es einen so genannten „verknüpften“ Klon, der als Daten-Cache gegenüber einem Snapshot der virtuellen Platte

aufgebaut wird. Dieser Snapshot wird dann als „gesperrt“, das heißt nicht löschbar, gesichert.

Aus diesem Grund ist das Klonen unabhängiger (independent) Festplatten, also persistenter oder nicht persistenter Platten, nicht möglich, da für diese keine Snapshots vorgesehen sind.

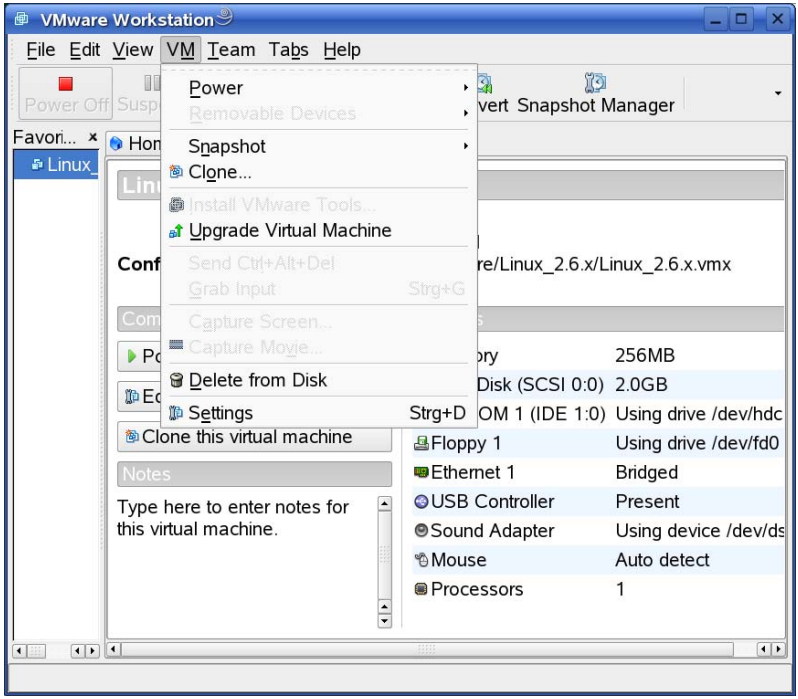


Abb. 7: Klone können über einen Dialog angelegt werden ...

Der verknüpfte Klon bleibt somit abhängig von der Master-VM, das heißt, er braucht dauerhaften Zugriff auf die Platten der Master-VM und verwendet lediglich für das Beschreiben der Platten einen Plattencache, der nun in einem gesonderten Verzeichnis abgelegt wird. Diese Eigenart verknüpfter Klone ist bei allen Nutzungsformen zu beachten, wo die Platten auf Dateisystemen gehalten werden, die nicht notwendig und immer gemeinsam verfügbar sind, zum Beispiel, wenn es sich um NFS-Verzeichnisse handelt.

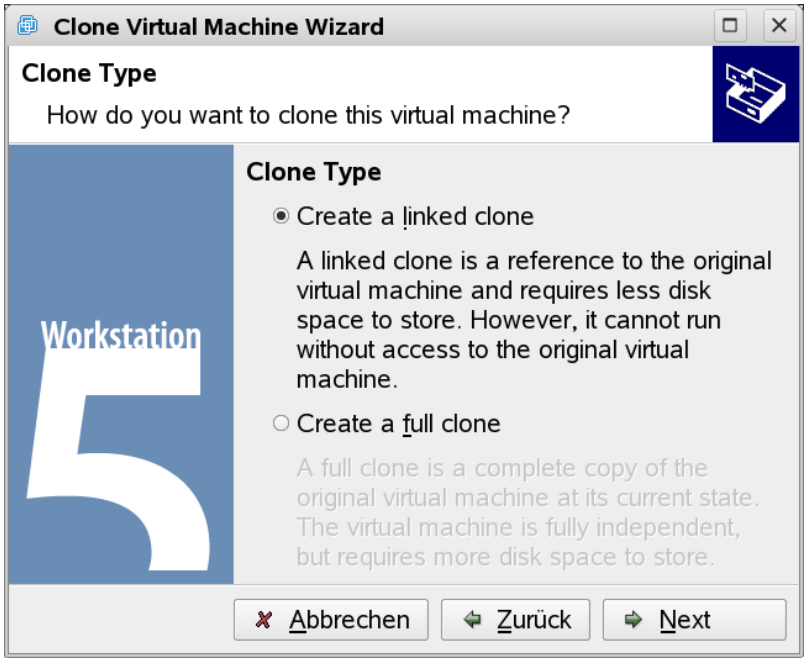


Abb. 8: ... in dem der Typ des Klon, vollständig oder verknüpfte, festgelegt werden kann.

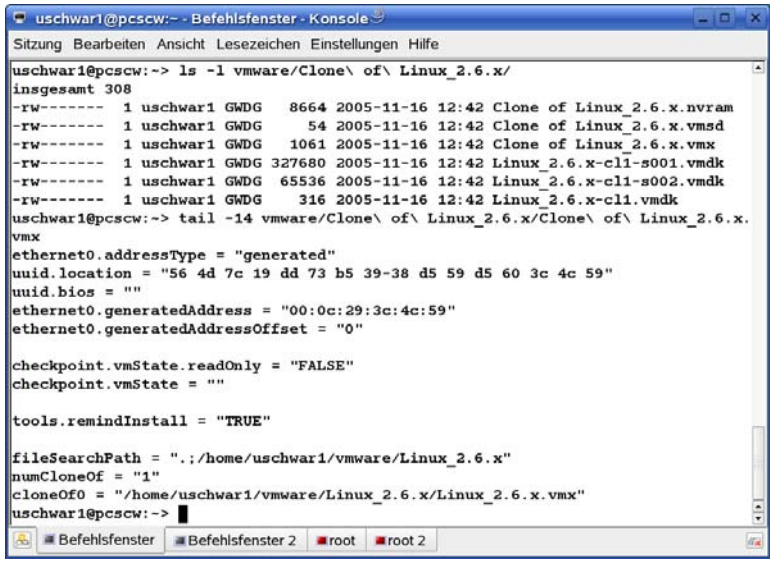


Abb. 9: Ohne weitere Snapshots ist die Dateistruktur des Klons noch übersichtlich. In der Konfiguration findet sich der Verweis auf die Herkunft.

Für die Verwaltung der Klone ist ein spezieller Wizard in VMware eingeführt worden, der den Ort festlegt, wo die Machine abgelegt wird und den Typ definiert. Er erzeugt den Klon vom gegenwärtigen Zustand, auch vor dem Start der Maschine, und legt den gesperrten Snapshot an.

Das Klonen von bereits existierenden Klonen ist erlaubt, was bei verknüpften Klonen allerdings zu der entsprechenden Leistungsverminderung führt, die die Umrechnung des Cachings von Platteninhalte mit sich bringt, die ihrerseit wiederum einem Caching unterliegen.

5. Teams

Ein weiteres wichtiges Konzept, das mit der Version 5 in VMware eingeführt wurde, ist das der Teams. Gemeint ist

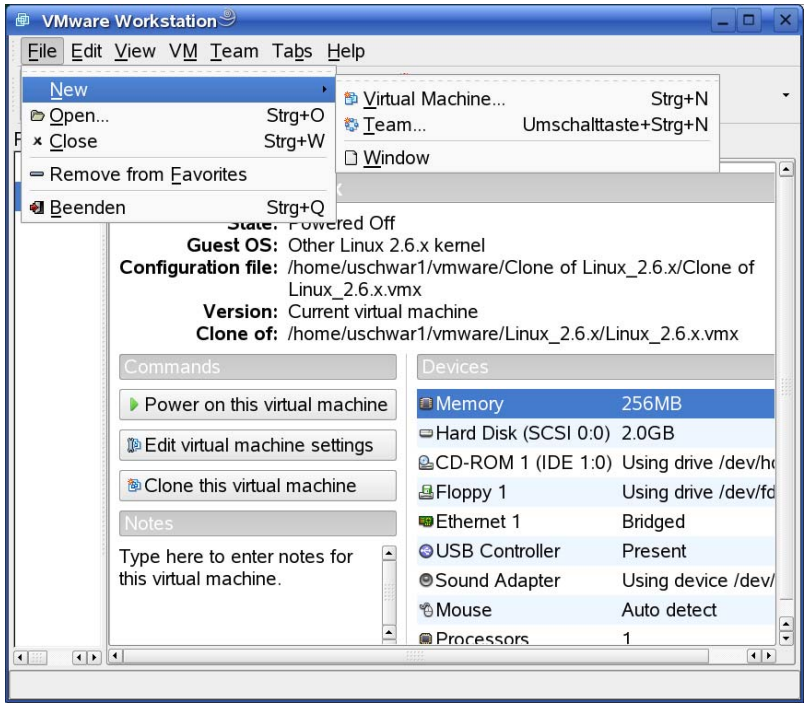


Abb. 10: Neue Teams lassen sich im Dialog konfigurieren.

damit die Organisation von Gruppen von VMs mit definierten Startabhängigkeiten und in eigenen Netzwerken. Diese Team-Netzwerke sind über LAN-Segmente definierbar, die zusätzlich zu den Schnittstellen eingeführt werden, die bereits aus vorangegangenen VMware-Versionen bekannt sind, wie die für das Bridged-, NAT- oder Host-only-Netzwerk.

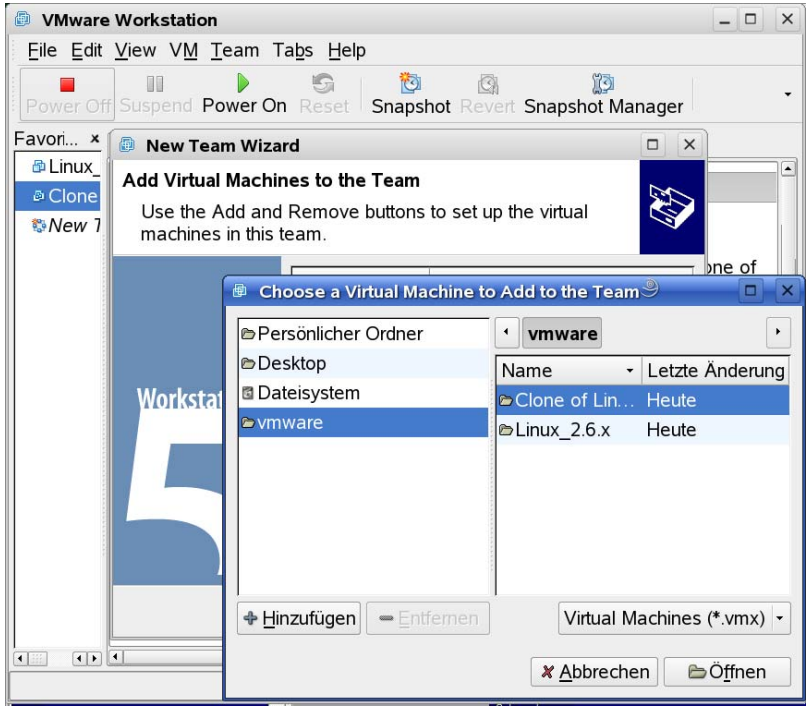


Abb. 11: Es werden VMs als neue oder bestehende Maschinen oder als Klone zum Team hinzugefügt.

Den Team-Mitgliedern können zusätzliche Ethernet-Adapter hinzugefügt werden, für die in den Team-Einstellungen die virtuelle Verknüpfung zu den gewünschten Schnittstellen festgelegt wird. Die LAN-Segmente wirken dabei so, als wären die Ethernet-Adapter über einen HUB miteinander verbunden. Es ist damit also das Verhalten von Maschinen in kleineren Netzwerke simulierbar, eine schöne Möglichkeit für viele Anwendungen.

Sollen grössere Netzwerke, Netzwerke mit Switches oder gar VLANs nachgebildet werden, ist dann der Einsatz des VMware-ESX-Servers, von dem dieses Konzept übernommen wurde, das Instrument der Wahl.

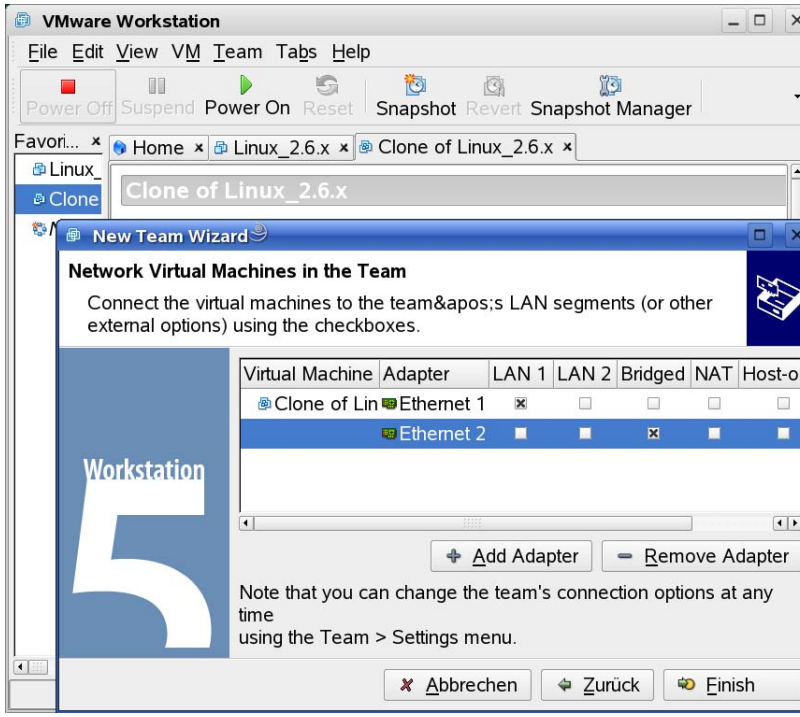


Abb. 12: Als wichtigste Eigenschaft von Teams lässt sich deren Zugehörigkeit zu LAN-Segmenten definieren.

Identity Management bei der GWDG

Sebastian Rieger

Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

1. Einleitung

Ziel des Projekts „Meta-Directory“ der GWDG ist es, die bestehenden Verzeichnisse und Datenbanken für die Verwaltung von Benutzern (bzw. Identitäten) innerhalb der GWDG zu synchronisieren. Hierbei wird eine Vereinfachung der Administration bzw. Verwaltung der Identitäten (Homogenisierung und Erhöhung der Qualität der Benutzerdaten) sowie der Anwendbarkeit durch die Benutzer („Self-Service“ ihrer Identitäten bzw. Benutzeraccounts, „Single Password“, teilweise „Single Sign-On“) angestrebt.

Zusammen mit weiteren Teilprojekten wie z. B. der Realisierung und Etablierung einer Public-Key-Infrastruktur für die Max-Planck-Gesellschaft und die GWDG [1] bildet das „Meta-Directory“, das bis Ende 2005 als Keyproject vorangetrieben wurde, eine Basis für die „einheitliche Authentifizierung“ auch über die Grenzen konkreter Systeme der GWDG, insbesondere im Göttingen-weiten GÖ*-Kontext (vgl. [2]), hinweg.

2. Meta-Directory als Basis für Identity Management

In der GWDG bzw. am Standort Göttingen allgemein existieren viele separate Verzeichnisse und Datenbanken für Benutzerkonten. Die Vielzahl der Verzeichnisse und Datenbanken begründet sich beispielsweise durch unterschiedliche Anwendungen oder Plattformen, die jeweils einen separaten Verzeichnisdienst oder eine gesonderte Datenbank für die Benutzerverwaltung verwenden. Um den Benutzern (bzw. Identitäten) zu allen Anwendungen und Ressourcen Zugang zu ermöglichen, müssen diese daher in allen Benutzerverwaltungen separat angelegt und gepflegt werden. Administrativ entsteht somit ein hoher Aufwand im Rahmen der Verwaltung bzw. des Identity Managements.

Führen die Benutzer ihrerseits Veränderungen an Ihren Benutzerdaten durch, so müssen sie diese in allen Verzeichnissen und Datenbanken separat nachtragen, um einen einheitlichen Stand der Daten zu erhalten. Beispiel hierfür ist die Änderung eines Passwortes, die an allen Systemen durchgeführt werden muss, um ein konsistentes Ergebnis zu erzielen.

Häufig werden zentrale Verzeichnisse basierend auf LDAP (vgl. OpenLDAP [3] oder Active Directory [4]) eingesetzt, um die Identitäten an einer Stelle zu verwalten und sie auf diese Weise zusammenzuführen. Begrenzt wird diese Integration allerdings durch Inkompatibilitäten der Anwendungen, Authentifizierungsverfahren und -systeme, die zudem häufig nur auf bestimmten Plattformen betrieben werden können. Die GWDG verwaltet daher ein zentrales Verzeichnis für ihre UNIX-Systeme (siehe auch [5]) sowie ein Active Directory für Windows-Systeme.

Um den Aufwand sowohl für die Administration als auch die Verwendung durch die Benutzer über zentralisierte und nach wie vor dezentrale Verzeichnisse und Datenbanken zu verringern, bietet sich eine automatisierte Replikation bzw. Synchronisation der Identitäten und zugehörigen Informationen an. Eine solche Synchronisation, wie in Abb. 1 illustriert, kann z. B. durch ein Meta-Directory erfolgen, das als Drehscheibe für die Identitäten und Attribute fungiert. Als externe Organisation neben der GWDG nennt die Abb. 1 den Geschäftsbereich 3-7 des Bereichs Humanmedizin der Universität Göttingen (GB 3-7 IT).

Das Meta-Directory erkennt Veränderungen in den Verzeichnissen und überträgt sie anhand definierter Kriterien und Regeln in die weiteren angeschlos-

senen Systeme. Hierbei werden die Informationen zusätzlich an das im jeweiligen Zielverzeichnis benötigte Format angepasst.

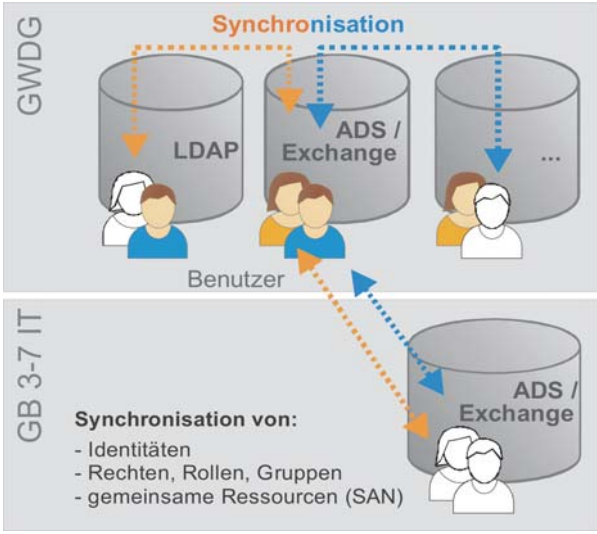


Abb. 1: Synchronisation von Identitäten über dezentrale Verzeichnisse

Die Synchronisation ermöglicht neben der einfacheren und effizienteren Administration und Verwendung auch den Abgleich von Passwörtern. Benutzer haben so die Möglichkeit ein einheitliches Passwort für die Verwendung der Anwendungen und Ressourcen zu verwenden („Single Password“). Dies steigert zusätzlich die IT-Sicherheit insbesondere bei der Vorgabe von Komplexitätskriterien für akzeptierte Passwörter (wie z. B. Länge, Sonderzeichen oder Passworthistorie), da die Benutzer mit zunehmender Anzahl von Passwörtern beginnen, diese aufzuschreiben (häufig in unmittelbarer Nähe ihres Rechners oder der verwendeten Ressource), direkt auf ihrem Rechner in der Anwendung abzuspeichern oder die Komplexitätskriterien (z. B. durch einen gezielten Überlauf der Passworthistorie) zu umgehen.

Zusätzlich können durch das Identity Management z. B. Rechte, Rollen und Gruppen für die der Authentifizierung folgende Autorisierung synchronisiert werden. Auch Daten für eine Nutzungsabrechnung (Accounting) nach erfolgreicher Authentifizierung und Autorisierung können abgeglichen werden. Insbesondere bei dezentralen und heterogenen IT-Strukturen ist jedoch die Bereitstellung der erforderlichen Infrastruktur für die Anwendung

wesentlich. Nach erfolgreicher Authentifizierung und Autorisierung soll der Benutzer beispielsweise Zugriff auf sein Home-Verzeichnis erlangen, was geeignete Verfahren für die Verfügbarkeit der Daten auch an dezentralen Systemen erfordert (z. B. durch eine geeignete SAN-Infrastruktur). Erst dann kann eine übergreifende und dezentrale Anwendungsbereitstellung, wie z. B. Göttingen-weit im Rahmen des GÖ*-Projekts geplant, erfolgen.

2.1 Synchronisation von Attributen und Identitäten

Der Fokus bei der Synchronisation von Identitäten und ihren zugehörigen Attributen liegt im Keyproject „Meta-Directory“ der GWDG auf dem Abgleich zwischen dem OpenLDAP-Verzeichnisdienst für UNIX-Systeme und dem Active Directory für Windows-Systeme. Anders als in vielen anderen Meta-Directory-Projekten, die mit großen Anlaufschwierigkeiten in der IT gestartet wurden, wird im Keyproject „Meta-Directory“ der GWDG ein pragmatischer Ansatz verfolgt, der nicht sofort alle Informationen und möglichen Datenquellen resp. Verzeichnisse synchronisiert, sondern sukzessive skaliert. Im Gegensatz zu vielen gescheiterten Projekten, die im ersten Schritt alle technischen Details fokussierten, kann so eine schrittweise organisatorische Planung von Abläufen bzw. der Synchronisation allgemein erfolgen, die eine weitaus größere Herausforderung als die technische Umsetzung darstellt.

Derzeit werden primär Organisationsstrukturen (Hierarchien mit Organisationseinheiten, z. B. Abteilungen), Benutzer und Passwörter abgeglichen. Zukünftig ist auch der Abgleich von Rechten, Rollen und Gruppen geplant.

Abb. 2 skizziert das Meta-Directory als Datendrehscheibe für die Attribute und Identitäten.

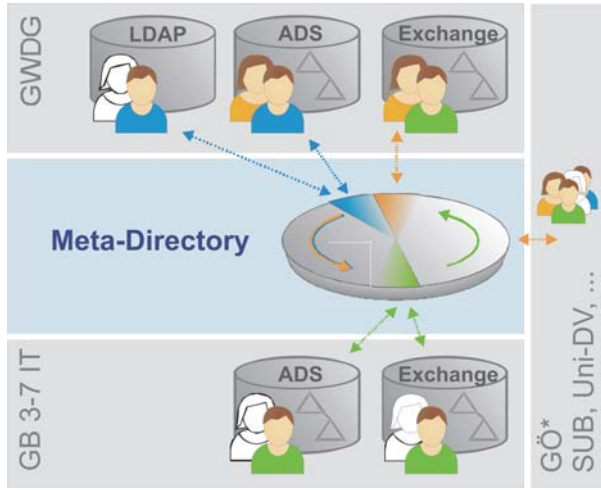


Abb. 2: Meta-Directory als Datendrehscheibe für Identitäten

Als initiale Quelle für die Fluss der Informationen resp. Attribute dient das OpenLDAP, das auch für die Anlegung neuer Benutzer bzw. deren Verwaltung durch das Keyproject „Benutzeraccount-Vergabe“ verwendet wird. Attribute wie beispielsweise Vor- und Nachname der Benutzer werden vom Meta-Directory nach festen Regeln in angeschlossene Zielsysteme übertragen und an die dortigen Anforderungen angepasst. Dadurch können zusätzlich Skripte, Individual-Lösungen und manuelle Synchronisation zugunsten einheitlicher sicherer Verfahren abgelöst werden.

Wie in Abb. 2 gezeigt, werden Identitäten beispielsweise direkt nach deren Erzeugung in relevante weitere Verzeichnisse und Datenbanken übertragen. So können beispielsweise neu angelegte Benutzer direkt auf ein Exchange-Postfach oder sowohl auf UNIX-Systeme, die OpenLDAP als Authentifizierungssystem verwenden, als auch auf Windows-Systeme am Active Directory zugreifen. Diese Synchronisation von Benutzern direkt nach deren Erzeugung wird auch als „Provisioning“ bezeichnet und umfasst zusätzlich das Starten von Workflows zur Einrichtung der benötigten Umgebung für die Benutzer, z. B. inkl. Rechte, Rollen und Gruppen.

Wird ein Benutzer als dem Quellsystem entfernt, so löscht das Meta-Directory bei Bedarf die synchronisierten Identitäten des Benutzers in allen ande-

ren angeschlossenen Systemen, was in Bezug auf die zusätzlich ausgelösten Prozesse z. B. zum Entfernen der Umgebung des Benutzers im Zielsystem auch als „Deprovisioning“ bezeichnet wird.

2.2 Synchronisation von Passwörtern

Einen Sonderfall bei der Synchronisation stellt das Passwort der Benutzer dar, da es i. d. R. in den Systemen individuell und in irreversibler Form verschlüsselt (als Hash z. B. nach MD5, SHA1 oder crypt) gespeichert wird. Es kann somit nicht für die Verwendung in zusätzlichen Zielsystemen bei der Synchronisation durch das Meta-Directory konvertiert werden.

Beim Identity Management werden daher i. d. R. web-basierte Portale verwendet, um das Passwort in allen geschlossenen dezentralen Systemen zu setzen. Dabei werden vom Meta-Directory passende Hash-Werte für die angeschlossenen Zielsysteme erzeugt. Entsprechende Portale bieten ggf. zusätzlich die Möglichkeit für den Benutzer, seine Identität resp. mit dem Benutzeraccount verknüpfte Attribute selbst zu ändern (Identity Management „Self-Service“).

Für die initiale Anmeldung am Portal bieten die Portale die Möglichkeit, bestehende Hash-Werte zu verwenden. Ebenfalls kann das Passwort direkt über zusätzliche Schnittstellen (z. B. direkt per LDAP) im Meta-Directory gesetzt werden. Dadurch können auch klassische Passwort-Änderungen von UNIX-Systemen via PAM (Plugable Authentication Modules) integriert werden.

Eine weitere Lösung bieten spezielle Filter, die das Passwort im Quellsystem vor der Erzeugung des zugehörigen Hash-Werts im Klartext abgreifen und asymmetrisch verschlüsselt an das Meta-Directory übermitteln. Diese Lösung wird beispielsweise durch spezielle Komponenten im Active Directory geboten.

Häufig werden die Passwörter im Meta-Directory in verschlüsselter Form, aber nicht als irreversibler Hash-Wert gespeichert. Auf diese Weise können sie in später zusätzlich angebundene Systeme, die beispielsweise neue Hash-Verfahren bzw. eine alternative Form zur Speicherung der Passwörter verwenden, übertragen werden. Wird diese Funktionalität geboten, so erfolgt die Speicherung im Meta-Directory i. d. R. mit einem administrator-sicheren Zugriffsschutz, so dass unberechtigten Dritten und regulären Administratoren kein direkter Zugriff auf reversibel verschlüsselte Passwörter geboten wird. Beispielsweise werden Hardware-Tokens (bzw. Crypto-Karten) oder geteilte Passwörter für die Administration des Systems verwendet.

Zur Berücksichtigung des Datenschutzes haben die Benutzer nach wie vor die Möglichkeit, in den einzelnen Systemen getrennte Passwörter zu verwenden, indem die Kennwörter direkt im Zielsystem gesetzt werden. Portale und Passwortfilter gehen jedoch voreingestellt von einer Synchronisation in alle angeschlossenen Verzeichnisse aus.

Die Abb. 3 zeigt die zeitnahe Synchronisation von Passwörtern über das Meta-Directory als Drehscheibe. Diese erfolgt in aller Regel in wenigen Sekunden und erhält Priorität vor anderen synchronisierten Attributen. Grundlage für diese Synchronisationsform stellt die Reaktion auf Ereignisse (Events) dar, so dass in diesem Zusammenhang auch von „event-basiertem“ Identity Management gesprochen wird.

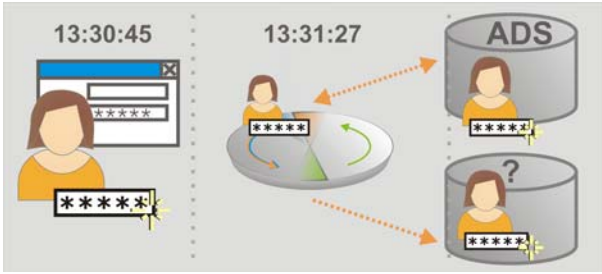


Abb. 3: Verteilung des Passworts in angeschlossene Systeme als „Event“

2.3 Einheitliche Identitäten

Neben dem Abgleich der Attribute und Passwörter einer Identität entsteht auch durch die Diversifikation der Benutzernamen ein Aufwand auf Seiten der Benutzer. Ideal wäre die Verwendung eines einheitlichen Benutzernamens in allen Anwendungen und Systemen. Dieser Anforderung stehen jedoch die zunehmend dezentrale Authentifizierung sowie technische Restriktionen der angebundenen Systeme gegenüber. So existieren beispielsweise in gängigen SAP-Systemen Längenbeschränkungen auf 12 Zeichen. Für die dezentrale Authentifizierung ist die Begrenzung der Gültigkeit bzw. Eindeutigkeit der Benutzernamen essentiell, um Namensdopplungen zu vermeiden.

Der Benutzername **`lmuelle`** (der fiktiven Benutzerin Lieschen Müller) dürfte ohne entsprechende Regelung nicht für den fiktiven Benutzer Lars Müller in einem anderen angeschlossenen System verwendet werden. Um für dieses Problem eine übergreifende, internationale Lösung z. B. für hohe Mobilität der Benutzer bzw. Roaming-Lösungen zu finden, haben sich im

Identity Management Benutzernamen basierend auf der E-Mail-Adresse etabliert (z. B. **`lmuelle@institut-a.gwdg.de`**). Die der Adresse angehängte Domäne dient hierbei als Realm (wie auch für Authentifizierungsverfahren wie Kerberos verwendet) und sorgt für eine weltweit eindeutige Bezeichnung. Neben der Länge des Benutzernamens, die die Bequemlichkeit der Eingabe einschränkt, lässt sich diese Lösung auch aufgrund der o. g. technischen Restriktionen der angeschlossenen Systeme derzeit nicht vollständig realisieren.

Basis für die spätere Vereinheitlichung der Benutzernamen bildet die Definition einer eindeutigen Bezeichnung der Identität im Meta-Directory, der mehrere Ausprägungen bzw. Benutzernamen in den Zielsystemen untergeordnet werden können. Durch die Verknüpfung der Benutzernamen wird eine spätere Migration zu einem einheitlichen Namen durch die entsprechende Synchronisation der angebundenen Systeme ermöglicht. Dies bedingt jedoch zusätzlich ein einheitliches Schema für die Informationen der Benutzer sowie bei Bedarf einheitliche Gruppen, Rollen und Rechte-Modelle.

2.4 Starten von externen Prozessen

Um nach erfolgreicher Authentifizierung und Autorisierung dezentral zur Verfügung gestellte Anwendungen nutzen zu können, müssen diese auf gemeinsame Ressourcen zurückgreifen können. Beispielsweise benötigt ein Benutzer nach erfolgreicher Authentifizierung Zugriff auf sein Home-Verzeichnis. Wird der Benutzer neu im System angelegt, so müssen dieses Home-Verzeichnis sowie weitere für die Anwendung notwendige Ressourcen angelegt werden. Für ein reibungsloses Arbeiten auf Seiten der Benutzer werden die Änderungen zeitnah als Ereignis, wie im vorherigen Abschnitt für Passwörter beschrieben, verarbeitet. Abb. 4 illustriert die Erzeugung eines E-Mail-Kontos inkl. Speicherplatz und Home-Verzeichnis beim Anlegen des neuen Benutzers.

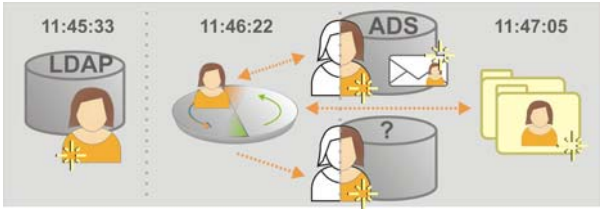


Abb. 4: Ausführung von externen Workflows / Skripten durch das Meta-Directory

Generell können Ereignisse wie z. B. Modifikationen, Löschungen oder das Anlegen neuer Benutzer externe Workflows z. B. über Skripte auf den Zielsystemen vom Meta-Directory gesteuert ausführen. Dabei werden den Aufrufen Parameter, z. B. die durchgeführten Änderungen oder relevanten Attribute, übergeben. Ausgaben der aufgerufenen Anwendungen können erneut ins Meta-Directory übernommen werden und neue Ereignisse auslösen (z. B. Abfrage des verfügbaren Speicherplatzes und bedingte Selektion eines alternativen geeigneten Speicherbereichs).

3. Integration von Public-Key-Infrastruktur, Single Sign-On und Federation

Identity Management umfasst mehr als die in den vorherigen Abschnitten beschriebenen Meta-Directory-Funktionen. Es umfasst die Verwaltung der Benutzeraccounts und zugehöriger Authentifizierungsinformationen von deren Erzeugung an. Daher kooperiert das Keyproject „Meta-Directory“ direkt mit dem Keyproject „Benutzeraccount-Vergabe“ der GWDG. Zusammen mit der Etablierung einer Public-Key-Infrastruktur (z. B. durch die Verwendung von Zertifikaten für unterschiedliche Anwendungen bzw. deren Integration auf Tokens) wie in [1] beschrieben, bildet es somit eine Basis für einheitliche Authentifizierung am Wissenschaftsstandort Göttingen.

Zukünftig wird die Integration in Föderationen (Identity Federation) mehr und mehr relevant. Diese ermöglichen eine dezentrale Nutzung und Single Sign-On für international verteilte Web-Anwendungen. Das Meta-Directory fungiert dabei als Identity Provider und stellt sog. Tokens aus, die als Sicherheitsmerkmal für die Authentifizierung an unterschiedlichen sog. Service Providern, die die gewünschte Ressource vorhalten, akzeptiert werden. Als Standard für die Definition der Tokens dient die Security Assertion Markup Language (SAML [6]). Ein Beispiel für die Verwendung von SAML im Federation-Umfeld ist Shibboleth [7].

Für Single Sign-On außerhalb von Web-Anwendungen existiert derzeit nur der „de facto“-Standard Kerberos [8]. Somit sind auch unter der Voraussetzung, dass Benutzername und Passwort einheitlich sind, für Anwendungen, die Kerberos nicht unterstützen, nach wie vor mehrfache separate Authentifizierungsvorgänge erforderlich. Verschiedene Identity-Management-Anbieter lösen dies u. a. durch Software-Clients, die auf den Arbeitsplätzen installiert werden, und beim Starten der jeweiligen Anwendung Benutzername und Passwort für den Benutzer eintippen. Das dafür notwendige Passwort beziehen sie in einer verschlüsselten Sitzung z. B. aus dem Meta-Directory (wie im vorherigen Abschnitt beschrieben). Diese Lösungen bie-

ten jedoch eine verminderte Sicherheit, sofern die Anwendungen und zugehörigen Passwort-Eingabe-Dialoge nicht eindeutig von der Software erkannt werden. Ein Beispiel für eine solche Lösung bietet die Fa. Novell mit dem Produkt Secure Login [9].

4. Implementierung bei der GWDG

Für den Einsatz im GÖ*-Umfeld wurden die Meta-Directory-Lösungen Microsoft Identity Integration Server [10], Novell Identity Manager [11] und Siemens DirX [12] evaluiert. Aufgrund des leichten funktionalen Vorsprungs wurde die Lösung der Fa. Novell für die Implementierung gewählt. Diese zeichnet sich durch eine flexible Passwort-Synchronisation anhand der o. g. Kriterien, eine dezentrale Administration des Systems, die einen kooperativen Betrieb ermöglicht, sowie eine gute Erweiterbarkeit z. B. um Single-Sign-On-Lösungen aus. Zusätzlich liefert die Lösung ein umfassendes Benutzer-Portal mit, das neben der zentralen Passwort-Verwaltung durch die Benutzer auch web-basierte Workflows und Identity Management Self-Services, wie eingangs beschrieben, bietet.

Die GWDG betreibt seit Oktober 2005 eine Testumgebung als „Proof-of-Concept“ des Novell Identity Manager. Gemeinsam mit der Fa. Novell Consulting wurde in dieser Umgebung die reibungslose Synchronisation von Benutzerkonten und Passwörtern implementiert. Dies ermöglicht es, am Standort, innerhalb des GÖ*-Projekts sowie in der GWDG Benutzer-Accounts (Identitäten) in verschiedenen Verzeichnissen und Datenbanken synchron anzulegen und zu löschen. Um die Administration wie auch die Anwendbarkeit für die Benutzer nachhaltig zu vereinfachen, repliziert das System auch die Passwörter gesichert über die angeschlossenen Systeme und vereinheitlicht somit die Authentifizierung der Benutzer. Später kann sukzessive auch der Abgleich z. B. von Adressverzeichnissen, Gruppen, Rechten und Rollen-Modellen über den Identity Manager erfolgen, wie erfolgreiche Tests bestätigt haben. Ermöglicht wird auch die Ausführung von Prozessen während der Verteilung der Benutzer, z. B. um Datenspeicher oder E-Mail-Postfächer anzulegen.

Neben der Testumgebung als „Proof-of-Concept“ wurde von der GWDG Ende 2005 ein Produktivsystem realisiert, das zunächst die ca. 33.000 Accounts (ca. 8.000 aktive Nutzer) der Internet-Hotline der Studierenden mit dem Active Directory der GWDG synchronisiert. Das Verfahren, das seit März 2006 produktiv eingesetzt wird, ermöglicht so den Nutzern der Internet-Hotline sowie der GWDG die einfache Verwendung von Arbeitsplätzen auf dem Campus (u. a. im Learning Resources Center (LRC) der SUB und der GWDG).

Erfahrungen bei der Integration der Identitäten aus der Internet-Hotline ermöglichen die für Quartal 3/2006 geplante Synchronisation von Identitäten aus dem GB 3-7 IT in das Active Directory der GWDG. Diese Accounts können dadurch die zentralen Exchange- und Active-Directory-Systeme der GWDG nutzen, und gleichzeitig eine eigenständige Active-Directory-Struktur mit individuellen Sicherheitsanforderungen unabhängig betreiben. Ab Quartal 3/2006 wird das Produktivsystem sukzessive um weitere angeschlossene Verzeichnisse erweitert.

Das Identity Management bzw. Meta-Directory der GWDG ist somit skalierbar ausgelegt und ermöglicht die langfristige Integration einer Vielzahl von Verzeichnissen am Wissenschaftsstandort Göttingen. Hierbei ist ein wesentlich kleinerer administrativer Aufwand für den Abgleich der Verzeichnisse notwendig, als über eigenständige und individuelle z. B. skript-basierte Lösungen. Nutzer und Administratoren können auf mehr Systeme einfach und zentral mit ihren bestehenden Benutzerdaten zugreifen. So wird nachhaltig auch die IT-Sicherheit gestärkt, da weniger Sonderlösungen existieren müssen und der Umgang mit Passwörtern vereinfacht wird.

Abb. 5 zeigt den derzeitigen Fluss der Identitäten im Eclipse-basierten Identity-Management-Werkzeug von Novell.

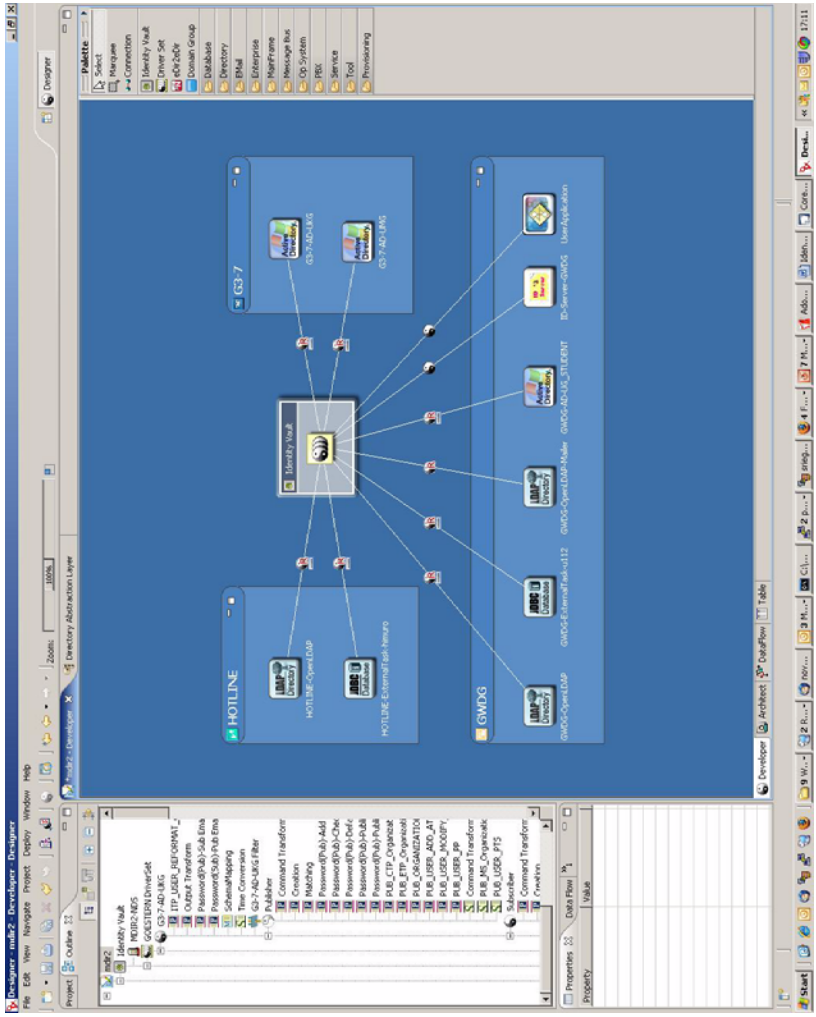


Abb. 5: Identity-Management-Benutzungsoberfläche

5. Status und zukünftige Planung

5.1 Abgeschlossene Meilensteine bzgl. der Implementierung der Test-Umgebung

- Die Produktauswahl wurde im November 2005 abgeschlossen:

  Novell, Siemens in Endausscheidung

  Novell Identity Manager wegen leichtem funktionalem Vorsprung als Meta-Directory-Lösung im GÖ*-Umfeld gewählt

  instanz-basierte Lizenz (pro gestartetem Meta-Directory), unabhängig von der Anzahl der Identitäten oder verwendeten Treiber

- Coaching von Novell Consulting für Umsetzung des „Proof-of-Concept“ zwischen GWDG und GB 3-7 IT

  Phase 1 (Okt 2005): Kick-Off und Integration OpenLDAP (UNIX)

  Phase 2 (Nov 2005): Integration Active Directory (Windows) / Exchange GWDG

  Phase 3 (Dez 2005): Integration Active Directory / Exchange GB 3-7 IT

- Benutzer- und Organisationsstrukturen werden synchronisiert
- Abgleich der Benutzer löst externe Prozesse (z. B. Anlegung von Verzeichnissen) aus
- Passwörter werden über Portal von Novell sowie aus den Systemen abgeglichen

5.2 Aktueller Status (Stand: Juni 2006)

- Die GWDG betreibt derzeit zwei Meta-DirectorySysteme (eine Testumgebung und ein Produktivsystem)
- Im Produktivsystem sind derzeit ca. 32.000 Identitätsobjekte von GB 3-7 IT des Bereichs Humanmedizin der Universität Göttingen, der GWDG und der Internet-Hotline für die Studierenden der Universität Göttingen vorhanden. Dies umfasst auch Identitätsobjekte (bzw. Benutzer) der Universität Göttingen sowie der Max-Planck-Gesellschaft allgemein.
- Innerhalb der GWDG wird der zentrale OpenLDAP-Server als führendes System z. B. mit Verzeichnissen des Mailers synchronisiert und es werden zentral Verwaltungsprozesse, Workflows und Skripte vom Meta-Directory gestartet.

- Die Synchronisation mit den Systemen des GB 3-7 IT ermöglicht hier den Abgleich der Benutzerkonten zwischen PatLAN und WissLAN im Universitäts-Klinikum.
- Die Integration des OpenLDAP-Servers der Internet-Hotline ermöglicht die Verwendung von Studierenden-Accounts z. B. für die Anmeldung am Active Directory der GWDG, wie sie im Learning Resources Center (LRC) in der Niedersächsischen Staats- und Universitätsbibliothek (SUB) angeboten wird.
- Für alle Benutzer steht ein zentrales Portal unter

  `http://benutzer-portal.gwdg.de`

  zur Verfügung, das neben dem zentralen Verwalten der Passwörter in den angeschlossenen Systemen auch delegierte Verwaltungsfunktionen sowie Self-Service für die Benutzer bietet. Hierzu folgt ein detaillierter Artikel in einer der nächsten Ausgaben der GWDG-Nachrichten.

5.3 Zukünftige Planung

- Im Quartal 3/2006 wird zusätzlich die Synchronisation der GB-3-7-IT-Benutzer zum Exchange-System der GWDG realisiert. Dies ermöglicht es den Benutzern, den Exchange-Service der GWDG zu verwenden, ohne eine weitere separate Benutzerverwaltung zu realisieren. Die Benutzerverwaltung verbleibt eigenständig im Active Directory des GB 3-7 IT und wird über das Meta-Directory synchronisiert.
- Der Abgleich mit dem Active Directory der GWDG wird Anfang Quartal 3/2006 abgeschlossen. Anschließend wird die Integration von externen Workflows im Active Directory z. B. für die Archivierung gelöschter Accounts realisiert.
- Erweiterungen um Verwaltungs-Workflows sowie Single-Sign-On-Lösungen insb. für Web-Anwendungen innerhalb der GWDG und in Kooperation mit der Medizinischen Informatik und der Niedersächsischen Staats- und Universitätsbibliothek sind geplant.
- Für die Quartale 3 u. 4/2006 ist geplant, die Anbindung weiterer Systeme (u. a. SAP und HIS der Universität Göttingen sowie ihres Bereichs Humanmedizin) zu realisieren.
- Um eine unterbrechungsfreie Synchronisation zu gewährleisten, wird im Quartal 3/2006 zusätzlich ein Redundanzystem als Meta-Directory im Rechenzentrum des GB 3-7 IT platziert.

6. Referenzen

[1] Rieger: PKI-Leistungen der GWDG. In: 21. DV-Treffen der Max-Planck-Institute; hrsg. v. Gartmann, Jähnke; GWDG-Bericht Nr. 67, 2005, S. 59 - 66

[2] Koke: Der Einfluss des GÖ*-Projektes auf die MPG. In: 19. und 20. DV-Treffen der Max-Planck-Institute; hrsg. v. Bussmann, Oberreuter; GWDG-Bericht Nr. 66, 2004, S. 65 - 79

[3] OpenLDAP:

http://www.openldap.org

[4] Active Directory:

http://www.microsoft.com/activedirectory

[5] Heuer, Ißleiber: LDAP in der GWDG - Einsatzspektrum. In: 21. DV-Treffen der Max-Planck-Institute; hrsg. v. Gartmann, Jähnke; GWDG-Bericht Nr. 67, 2005, S. 53 - 58

[6] Security Assertion Markup Language:

http://www.oasis-open.org/committees/security

[7] Shibboleth:

http://shibboleth.internet2.edu

[8] Kerberos:

http://web.mit.edu/kerberos

[9] Secure Login:

http://www.novell.com/securelogin

[10] Microsoft Identity Integration Server:

http://www.microsoft.com/miis

[11] Novell Identity Manager:

http://www.novell.com/idm

[12] Siemens DirX:

http://www.siemens.com/index.jsp?sdc_p=
t4cz3s4u0o1180841pHPnfl0mi1077887

Intrusion Detection und Prevention im GÖNET

Andreas Ißleiber

Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

1. Einleitung

In den letzten Jahren haben sich IDS und IPS zu einem festen Bestandteil der Sicherheitsinfrastruktur entwickelt. IPS und IDS schließen eine wesentliche Lücke zwischen meist schon vorhandenen Firewalls und Virenscannern.

Für einen ausreichenden Schutz des GÖNET sind bereits an den zentralen Standorten leistungsfähige Firewallsysteme integriert (vgl. die GWDG-Nachrichten 2/2006). Überdies steht ein reichlich genutztes Angebot an Virenscannern zum Schutz der lokalen Systeme in den Instituten zur Verfügung. Dennoch existiert eine Bedrohungslage, die für den Benutzer nicht leicht zu erkennen ist. Attacken und Eindringlinge werden i. d. R. nicht durch Firewalls und Virenscanner erkannt und entsprechend bekämpft. Ausgenutzte Sicherheitslücken der Betriebssysteme führen häufig zu einer Kompromittierung des eigenen Rechners, oft auch über einen längeren Zeitraum und häufig vom Benutzer unbemerkt. In der Folge werden diese Rechner dann selbst zu einer Quelle diverser Attacken innerhalb des eigentlich sicheren Netzwerkes. Die von der GWDG erhobenen Statistiken hinsichtlich Attacken und Angriffen im GÖNET zeigen zwar einen positiven Einfluss als Folge der Integration der GÖNET-Firewalls, machen aber auch deutlich,

dass die Anzahl subtiler und komplexer Attakken und Angriffe durch die bestehenden Komponenten allein nicht zu reduzieren ist.

Genau an dieser Stelle entsteht ein Bedarf an mehr Sicherheit, welcher durch den Einsatz eines IPS/IDS gedeckt werden kann.

2. Anforderungen und Motive für ein IPS/IDS

Die Anforderungen an einen so komplexen Sicherheitsmechanismus sind nicht gering. Für die Auswahl eines geeigneten Systems sind für die GWDG die folgenden Merkmale entscheidend:

- **Absicherung des lokalen Netzwerkes**

  Ein IDS/IPS soll in erster Linie das lokale Netzwerk vor Attacken schützen.

- **Automatische Abwehr**

  Um den Wartungsaufwand für ein solches System gering zu halten, sollte es nach Möglichkeit angemessen und vollständig autonom auf etwaige Bedrohungen reagieren, ohne das ein Administrator eingreifen muss.

- **Über Bedrohungen benachrichtigen**

  Entscheidend ist auch die Benachrichtigung über die erfolgte Abwehr von Attacken. Überdies sollten alle Ereignisse in einem geeigneten Verfahren mitprotokolliert werden können (Logging).

- **Hohe Bandbreite**

  Damit ein IPD/IDS den Datenverkehr nicht stört oder beeinträchtigt, muss es eine dem Netzwerk angepasste Bandbreite besitzen. Im GÖNET wird an den entscheidenden Knotenpunkten mit Bandbreiten von 1 GBit/s gearbeitet. Diese Bandbreite muss ein IPS beherrschen.

- **Schnelle Reaktion auf neue Bedrohungen sowie hohe Erkennungsrate**

  Die Qualität der Erkennung von Attacken ist das wesentliche Merkmal für ein IPS/IDS. Da nahezu täglich neue Varianten diverser Attakken auftreten, muss ein IPS diesem Umstand Rechnung tragen und sich entsprechend schnell an die immer wieder neue Bedrohungslage anpassen.

- **Einfaches Management**

  Das System sollte eine Managementumgebung mitbringen, mit der auch Nicht-Netzwerkexperten eine Einschätzung der Gefahrensituation

erlaubt. Überdies sollte das IPS in eine standardisierte Managementumgebung integriert werden können und eine automatische Alarmierung bei Notsituationen erlauben.

Die Motive sind klar. Um sich vor weniger auffälligen und von den bisherigen Sicherheitseinrichtungen wie Firewall und Virenscannern nicht zu erkennenden Angriffen schützen zu können, muss eine neues System im Netzwerk integriert werden, welches speziell für diesen Zweck geschaffen wurde. Erfolgreiche Angriffe auf Rechner im GÖNET können erheblichen Schaden anrichten, wenn von dem befallenen System weitere Rechner attakkiert werden.

3. Was ist ein IDS?

Die grundlegende Aufgabe eines IDS (Intrusion-**Detection**-System) ist die Erkennung von

- Attacken und
- abnormalen Verhalten im Netzwerk.

Anders als Firewalls versuchen IDS/IPS den Netzwerkverkehr auf den höheren Protokollschichten zu analysieren. Das wird in der Praxis bis zur Anwendungsschicht (Layer 7) realisiert. Über die Analyse des Datenverkehrs und das Vergleichen mit bekannten Angriffsmustern und Signaturen versuchen IDS Attacken zu erkennen. Ein IDS muss demnach so angeordnet sein, dass es den zu überwachenden Datenstrom „mitlesen“ kann. Hierbei werden die Systeme nicht unmittelbar in den Datenstrom integriert, sondern vielmehr parallel zum Datenstrom angebunden. Dieses kann häufig über Switches erreicht werden, bei denen ein bestimmter Port als „Monitoring“-Port eingestellt werden kann. Über diesen Monitoring-Port wird der Datenstrom parallel zum IDS geleitet, der wiederum die Netzwerkpakete auf Attacken und Unregelmäßigkeiten untersuchen kann. Eines der Probleme bei dieser Variante ist die Tatsache, dass bei einem Ethernet-Switch mit mehreren Ports nur ein Port für das Monitoring genutzt werden kann und dadurch nicht der gesamte über den Switch laufende Traffic über diesen Port sichtbar ist.

Nehmen wir einen 24-Port-FastEthernet-Switch mit 100 MBit/s pro Port. Wenn der Switch nur zur Hälfte auf allen anderen Ports ausgelastet ist (23 x 50 MBit/s = 1,18 GBit/s), kann der resultierende Gesamttraffic unmöglich auf dem einen 100-MBits/s-Monitoring Port ausgegeben werden. Deshalb sind meistens nur direkte Port-Paarungen möglich. Nur ein Port kann zu einem Monitoring-Port gespiegelt werden. Durch geschickte Auswahl des zu

überwachenden Ports kann jedoch häufig eine Überwachung der entscheidenden Netzwerkdaten gelingen.

Für IDS ist es auch nicht unbedingt relevant, jedes Paket mitlesen zu können. Häufig genügt es, nur einen Teil des Netzwerkverkehrs zu überprüfen, basierend auf der Annahme, dass eine Attacke mehrfach vorkommt und die Wahrscheinlichkeit der Erkennung mit der Häufigkeit der Attacke wächst. Das trifft insbesondere bei (D)DOS-Attacken (DOS = Denial of Service) zu, die oft mit hohen Datenaufkommen einhergehen. Ein vollkommener Schutz vor Angriffen ist bekanntlich nicht möglich, so dass viele Systeme sich auf die Erkennung der wesentlichen Attacken beschränken.

Dennoch gibt es Angriffe, die nur aus einem einzigen Netzwerkpaket resultieren und dadurch oft nicht von einen IDS erfasst werden.

Die folgende Abb. 1 stellt eine typische Integration eine IPS im Netzwerk dar:

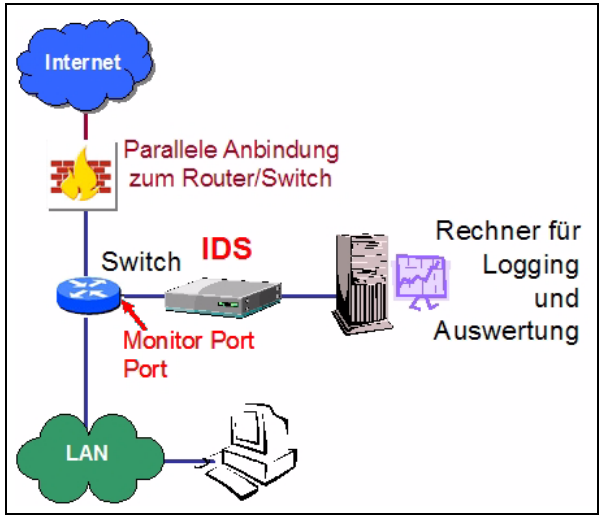


Abb. 1

Der entscheidende Nachteil im Vergleich zu einem IPS ist die Tatsache, dass Angriffe zwar protokolliert werden, aber keine automatische Gegenabwehr eingeleitet wird. Ein IDS ist ein passives Überwachungssystem und daher vergleichbar mit einem „Wolf ohne Zähne“. Mit dem Einsatz eines IDS geht ein außerordentlich hoher Administrationsaufwand einher. Bei jeder Attacke bleibt es dem Administrator überlassen, welche Maßnahmen einzuleiten sind. Wenn man sich die Vielzahl der Attacken aus dem Internet in das

GÖNET ansieht, wird schnell klar, dass der Einsatz eines IDS als alleiniges System zur Verhinderung von Angriffen nicht beherrschbar ist.

Uns erreichen im GÖNET täglich zwischen 1.000 und 100.000 Attacken von einigen Hundert bis einigen Tausend verschiedenen Quellen. Ein Administrator mit dem IDS als Werkzeug ist diesem Umstand hilflos ausgeliefert. Überdies ist auch die Gegenabwehr bei Attacken nicht trivial, wenn diese manuell erfolgen muss. Oft bleibt dem Administrator nur das „Unterbrechen“ der Kommunikationsbeziehung zwischen Angreifer und Opfer. Ist der Angriff eine (D)DOS-Attacke, wird das Szenario schnell zu einem Desaster, da die Angriffe aus vielen Quellen kommen.

4. Was ist ein IPS?

Die Fähigkeiten des IDS sind auch bei einem IPS (Intrusion-**Prevention**-System) zu finden. Es entdeckt Attacken sowie abnormales Verhalten. Der entscheidende Unterschied ist aber die von einem IPS ausgehende automatische Gegenabwehr bei Angriffen. Der Datenstrom wird beim IPS in gleicher weise überwacht. Wird ein Angriff identifiziert, kann ein IPS die Kommunikationsbeziehung entweder vollständig unterbrechen oder nur die entscheidenden schadhaften Netzwerkpakete herausfiltern, indem die TCP- oder UDP-Verbindung für die benutzten (TCP/UDP)-Ports unterbrochen wird. Nützlicher bzw. gewünschter Datenverkehr kann so vom schadhaften Traffic isoliert werden.

Die folgendes Abb. 2 verdeutlicht den Einsatz eines IPS im lokalen Netzwerk:

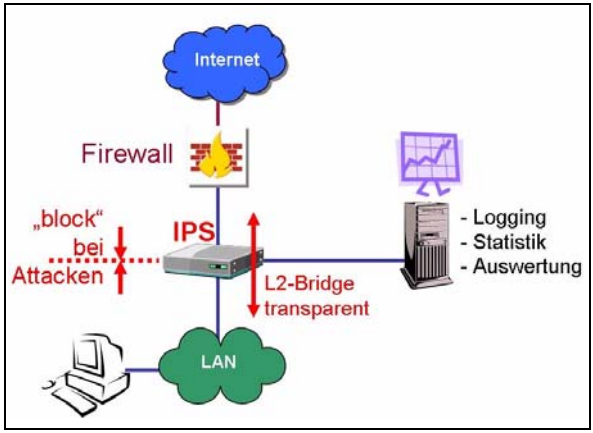


Abb. 2

Durch ein IPS kann aufgrund der automatisierten Abwehr von Attacken der administrative Aufwand im Vergleich zum IDS ganz erheblich reduziert werden, im Idealfall bis hin zu einem vollkommen autonomen System nahezu ohne manuellen Eingriff. Die Zeit zwischen der Erkennung der Attacke und der Gegenabwehr ist beim IPS auf ein Minimum reduziert.

Ein IPS muss gute Filter haben!

Funktionsbedingt muss die Qualität der Erkennung bei einem IPS im Vergleich zum IDS erheblich höher sein. „False Positive"-Erkennung, also die Bewertung von legalem Traffic als Attacke, hat bei einem IPS viel weiterreichendere Konsequenzen als bei einem IDS, da die Verbindung automatisch blockiert werden würde. Sind Lücken oder Schwächen bei der Erkennung eines IPS bekannt, könnten diese quasi als DOS-Angriff zweckentfremdet werden. „False Positives" sollten demnach bei einem IPS nicht auftreten, was zwar nicht immer der Realität entspricht, aber dennoch von vielen Systemen annähernd erreicht wird.

5. Vergleich IPS/IDS

Wenngleich die enge Verwandtschaft zwischen IPS und IDS deutlich ist, existieren aufgrund des entscheidenden Unterschieds gravierende Vor- und Nachteile beim direkten Vergleich der Systeme.

Die folgende Tabelle vergleicht IPS und IDS:

IDS	IPS
Vorteil: • Einsatz mehrerer Sensoren im Netz	Vorteile: • aktive Abwehr von Angriffen • geringerer administrativer Aufwand
Nachteile: • Überwachung des IDS durch Administrator erforderlich • manuelle Reaktion auf Attakken erforderlich • (zu) viele Logginginformationen	Nachteile: • im inline-mode: schnelle Erkennung und Reaktion erforderlich • teure Hardware, d. h. hoher Preis

6. Diverse „Typen“ von IDS und IPS

IDS sowie IPS können in verschiedenen Konfigurationen im Netzwerk integriert werden. Es lassen sich zwei grundlegend unterschiedliche Klassen unterscheiden:

1. Hostbasierte IDS/IPS (HIPS)

Kleinere Formen eines IDS/IPS sind bereits in einiger Antivirensoftware als Ergänzung zu finden. Hostbasierte Systeme sind immer auf einem Rechner als Software installiert und schützen damit auch ausschließlich das lokale System. Der entscheidende Vorteil ist die Erkennung von schadhaften Prozessen auf dem eigenen Rechner (RootKits etc.). Ein zentrales IPS kann nicht die Prozesse eines Betriebssystems erkennen und ggf. schützen.

2. Netzbasierte IDS/IPS (NIPS)

Netzbasierte IPS werden an zentraler Stelle im Netzwerk platziert. Sie schützen im Vergleich zum „HIPS“ ein gesamtes Netzwerksegment und sind weniger auf den Schutz des einzelnen lokalen Host fixiert.

Eine Kombination aus beiden Varianten ist durchaus denkbar, um die Vorteile beider Systeme nutzen zu können.

Die folgende Tabelle verdeutlicht die Vor- und Nachteile beider Verfahren:

Hostbasierte IPS (HIPS)	**Netzbasierte IPS (NIPS)**
Vorteile: • geringe Datenmenge, Bandbreite • Systemzustand auf Rechner erkennbar, „schädlicher Code“ • bei „false positive“ nur eigenes System betroffen	Vorteile: • kann ganzes Segment überwachen/schützen • besserer Schutz bei (D)DoS-Attacken • Überblick über gesamtes Netz (Gesamtbild ergibt erst eine Attacke) • sieht auch Attacken auf unbenutzten Adressen • zentrales Management

Hostbasierte IPS (HIPS)	Netzbasierte IPS (NIPS)
Nachteile: • ggf. auf OS-Ebene auszuhebeln, da Programm/Dienstbasierend • Verwaltung pro Host (Aufwand) • eingeschränkte Sicht (nur eigener Host)	Nachteil: • hohe Bandbreite (erforderlich) und damit verbundene Latenzen

7. Auswahl des geeigneten Systems

Die GWDG hatte für die Auswahl eines für das GÖNET geeigneten IDS/IPS verschiedene Produkte entweder im Test oder deren Fähigkeiten im Rahmen einer Produktstudie analysiert. Nahezu alle großen Netzwerkhersteller haben auch ein IPS im Produktportfolio. Gelegentlich sind es nur Erweiterungen bereits bestehender IDS, die durch Titelkosmetik und leichte Modifikationen zu einem IPS erweitert wurden. Abhängig davon, aus welchem Bereich der Hersteller kommt, besitzen die IPS entsprechende Stärken und Schwächen. Cisco, Enterasys, 3COM sowie Fortigate kommen aus dem Netzwerkbereich. McAffee stammt klassisch aus dem Bereich der Virenerkennung. Oft ist das Knowhow durch Zukauf einer Firma in die eigene Produktpalette des Herstellers gelangt (Bsp.: 3COM und McAffee) oder wurde durch Partnerschaften ergänzt (Bsp.: Cisco & McAfee).

Auch die Fähigkeiten des OpenSource-Produktes „Snort“ wurde als Alternative im Rahmen einer Testinstallation bei der GWDG untersucht.

Genauer betrachtet wurden:

Produkt	Grundlage der Bewertung
1. **Cisco IDS/IPS**	Bewertung durch Vorführung von Cisco sowie Besuche von Cisco-Partnern bei der GWDG
2. **McAfee** (Intrushield als Appliance)	Im Rahmen mehrerer Vorstellungen von McAffee bei der GWDG bewertet

Produkt	Grundlage der Bewertung
3. **Fortigate** (Fortinet: Firewalls mit IDS/ IPS-Zusatz basierend auf Snort in einer Appliance)	Vorstellung des Herstellers bei der GWDG sowie kurze 10-tägige Testphase im Rahmen der Firewallauswahl bei der GWDG
4. **Snort** (OpenSource)	Testphase im lokalen Netz sowie Schulung im Rahmen des DV-Treffens der Max-Planck-Institute 2005
5. **Dragon von Enterasys (IDS)**	Als Appliance; Betrieb bei der GWDG 2004
6. **Tippingpoint (3COM)**	Bewertung im Rahmen eines 14-tägigen Tests bei der GWDG.

8. Die Ergebnisse im Überblick

Ganz entscheidend für den Einsatz eines IPS im GÖNET ist die Bandbreite des Systems. Viele Produkte schieden allein aufgrund der geringen Performance aus. Immerhin verfügt die GWDG über eine Internetanbindung von 1 GBit/s. Ein System musste in der Lage sein, diese Bandbreite ohne nennenswerte Beeinträchtigungen für die Benutzer zu bedienen. Klar war überdies, dass ein reines IDS aufgrund der nicht vorhandenen Mechanismen zur Gegenabwehr und des hohen Administrationsaufwands nicht in Frage kommt.

1. Die **Cisco**-IPS-Lösung war Bestandteil eines großen Sicherheitskonzeptes mit dem Namen „Cisco Self-Defending Network“. Hier wurde ein IDS/IPS als Sensor im Netzwerk platziert und meldeten einer zentralen Einrichtung die Ergebnisse, die wiederum mit weiteren Ergebnissen aus Logfiles und Ereignisanalyse weiterer Systeme zu einem Gesamtbild korreliert werden. Der entscheidende Nachteil dieser Lösung in Hinblick auf die derzeitige Struktur im GÖNET war die Tatsache, dass das Gesamtsystem ausschließlich Cisco-Komponenten erwartet. Systeme anderer Hersteller wurden, wenn überhaupt, nur sehr unzureichend unterstützt. Darüber hinaus konnten andere Systeme in der Erkennungsleistung mehr überzeugen.

2. **McAfee**(s) Intrushield-Ansatz sah zunächst sehr vielversprechend aus. Hier werden nur Dinge überprüft, die auch wirklich eine Gefahr für die

Rechner darstellen. Eine IIS(Internet Information Server)-Attacke auf einen Apache-Webserver bleibt in der Regel folgenlos und ist damit für das Erkennungssystem von geringem Interesse. Der Nachteil dieser Lösung lag in der geringeren Bandbreite. Für die Analyse von Datenströmen von 1 GBit/s an mehreren Stellen im GÖNET gleichzeitig war das System nicht ausgelegt.

3. Fortinets **Fortigate**-Lösung ist primär eine Firewall mit einem IPS als „AddOn“. Da die GWDG sich bei der Auswahl einer geeigneten Firewalllösung im GÖNET für Cisco entschiedenen hatten (vgl. die GWDG-Nachrichten 2/2006), ist ein wesentliches Argument hinsichtlich einer einheitlichen Gesamtlösung nicht mehr vorhanden. Überdies hatte Fortigate lediglich eine angepasste Snort-Lösung in den Firewalls integriert, welche die geforderte Bandbreite nicht erreichte.

4. **Snort** als einziges OpenSource-Produkt im Test ist primär ein IDS. Bereits 1998 waren erste Snort-Varianten verfügbar. Erst später kamen Mechanismen hinzu, unerwünschte Verbindungen aktiv zu beenden (TCP-Reset etc.). Gerade dieser Bereich ist aber im Vergleich zu einigen kommerziellen IPS-Lösungen noch nicht so weit entwickelt, so dass ein Einsatz im GÖNET als einziges IPS nicht sinnvoll erscheint. Dennoch hat Snort eine sehr große Verbreitung gefunden. In Verbindung mit kommerziellen Systemen wäre der Einsatz von Snort als „Sensor“ im GÖNET durchaus denkbar. Aufgrund der großen „Community“ findet bei Snort eine ständige, unter OpenSource stehende Weiterentwicklung statt, obwohl Snort auch einen kommerziellen Zweig besitzt. Die damaligen Snort-Entwickler hatten eine eigene Firma namens „Sourcefire“ gegründet.

   Ein weiteres im OpenSource-Bereich angesiedeltes IPS ist „**Hogwash**“ (`http://hogwash.sourceforge.net`). Im Vergleich zu Snort ist es als IPS konzipiert worden. Bei der Bewertung der Einsatzfähigkeit im GÖNET treffen aber die gleichen Kriterien zu wie bei Snort.

5. Enterasys **Dragon** schied von vornherein aus, da es sich lediglich um ein IDS handelt.

6. **Tippingpoint (3COM)** ist ein spezialisierter Hersteller von IDS/IPS gewesen, welcher von 3COM aufgekauft wurde und als eigene „Division“ bei 3COM unter dem alten Namen firmiert. Das System wurde der GWDG Ende 2005 von 3COM vorgestellt. Im Anschluss daran konnte wir das Tippingpoint-System für etwa drei Wochen im Einsatz bei der GWDG getestet werden. Aufgrund der Ergebnisse dieser Tests und der Vergleiche mit den anderen Lösungen hatte die GWDG sich für das Tip-

pingpointsystem als zentrales IPS entschieden. Nicht zuletzt der sehr erfolgreiche Test bei der GWDG und die sehr hohe Bandbreite waren ausschlaggebend für diese Entscheidung. Das System lässt sich als vollkommen transparentes Gerät in den Datenstrom integrieren und ermöglicht damit einen sehr unkomplizierten Einsatz im GÖNET.

Die Wahl eines für das GÖNET geeigneten IPS fiel zugunsten der Firma Tippingpoint (3COM). Nicht nur die hohe erreichbare Bandbreite, sondern auch das einfache und überschaubare Management des Gesamtsystems waren ausschlaggebend für die Auswahl des Produktes.

9. Das IPS von Tippingpoint

Tippingpoint hat unterschiedliche Systeme im Produktportfolio, die sich in Bezug auf IPS im Wesentlichen in der Bandbreite und der Anzahl der Ports unterscheiden. Das für die GWDG geeignete Gerät ist das „Tippingpoint 2400 E“ (s. Abb. 3), welches sich seit Anfang Dezember 2005 bei der GWDG im produktiven Einsatz befindet.

Abb. 3

Die IPS von Tippingpoint arbeiten vollständig transparent. Das Gerät wird in den Kommunikationsweg installiert, sodass die Kommunikationspartner das IPS im Netzwerk nicht wahrnehmen. Die Netzwerkpakete werden vom IPS unverändert an den jeweils anderen Port weitergeleitet, solange in dem Datenstrom keine Attacke enthalten ist. Das IPS 2400 arbeitet bidirektional, sodass die Richtung einer etwaigen Attacke für das System keine Rolle spielt. Angriffe werden damit in beide Richtungen erkannt und entsprechend unterdrückt.

Die Features des IPS 2400 E sind:

- Bandbreite: 2 GBit/s
- vier Gigabit-Doppelports
- Kombination aus Hardware & Software (Management)
- Failover-Betrieb (Hot Standby)

- diverse Eventkategorien (Minor bis Critical)

9.1 Aufbau der Tippingpoint-Lösung

Die IPS-Hardware

Das Tippingpoint besteht aus zwei Komponenten: Zunächst werden durch das eigentliche IPS-Gerät der Datenverkehr analysiert und bei Attacken bestimmte Ereignisse ausgelöst. Dieses System besitzt mehrere spezielle Netzwerkprozessoren, um die hohe Bandbreite bei der Analyse der Datenpakete zu gewährleisten. Das IPS 2400 E besitzt vier Gigabit-Doppelports, die vollständig transparent arbeiten.

Das Managementsystem SMS

Ein vom IPS abgesetzter Server beinhaltet eine spezielle Managementsoftware, über die das IPS kontrolliert wird. Es heißt „SMS“ (Security Management System) und besteht aus einem Dell-Server und einer für das Management angepassten Software, die eine Bedienung des Systems entweder über eine Webseite oder einen Client erlaubt. Überdies sammelt das SMS alle Ereignisse und speichert diese für weitere Auswertungen in einer internen SQL-Datenbank. Gleichzeitig werden vom SMS automatisch Alarme generiert, wenn bestimmte Ereignisse eintreten. Nicht zuletzt auch das Firmware-Management wird vom SMS übernommen sowie die täglichen Updates an Signaturen für bekannte Attacken.

So sind zwei wesentliche Komponenten auf die zwei Systeme verteilt: Dell-Server sowie IPS-Hardware. Das IPS selbst kann sich damit auf die zeitkritische Analyse der Pakete konzentrieren.

9.2 Attacken erkennen, aber wie?

Die Signaturen

Eine der Verfahren zur Erkennung von Angriffen ist der Vergleich der Datenpakete mit bekannten Signaturen. Der größte Teil der Attacken lässt sich über signaturbedingte Filter erkennen, wenngleich nicht alle. Eine große Anzahl an Personen analysieren täglich neue Angriffe und Eindringlingsversuche und generieren daraus Muster, auf deren Basis dann Filter für IPS erzeugt werden. Mit dem Kauf des Tippingpoint-Systems besteht zugleich auch ein Updatevertrag, auf dessen Basis fast täglich neue Signaturen automatisiert auf das System geladen werden, um bei neuen Angriffswellen diesen möglichst schnell begegnen zu können. Tippingpoint nennt diese Signaturupdates sehr treffend „Digital Vaccine“.

Die Gesamtzahl der Signaturen beläuft sich derzeit auf 2.700 - 3.000. Das IPS unterscheidet auch den Schweregrad der Attacke und aktiviert in dessen Abhängigkeit entsprechende Abwehrmaßnahmen.

Unterschieden werden folgende Einteilungen:

- Minor
- Major
- Critical

Abb. 4 zeigt ein Beispiel (Auszug aus den Signaturen des IPS):

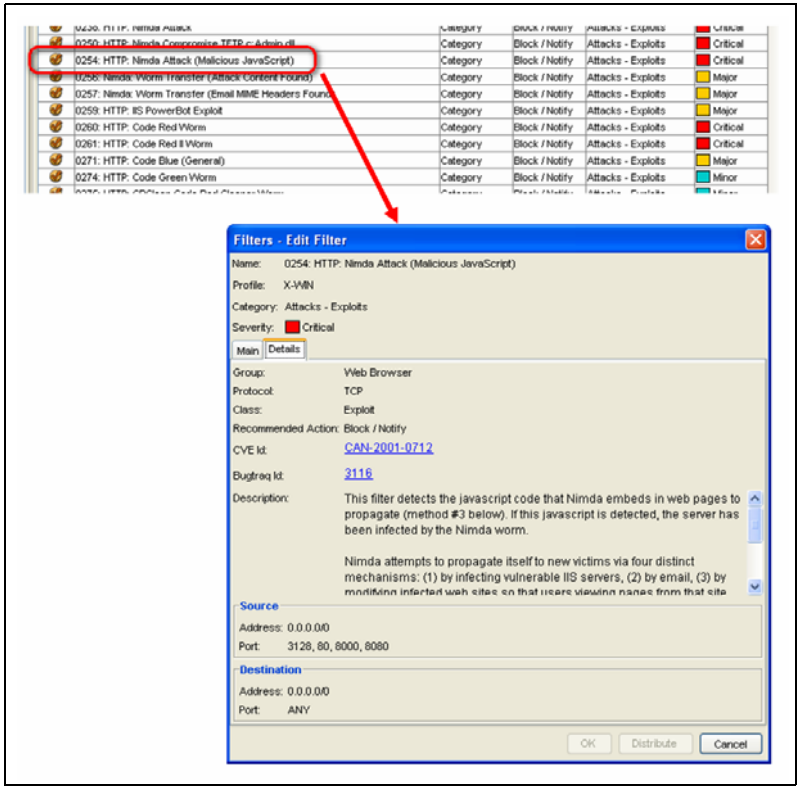


Abb. 4

Jede Signatur besitzt eine interne, eindeutige Tippingpoint-Nummer und basiert auf international eindeutigen Kennnummern für bekannte Attacken.

Das IPS (bzw. SMS) gibt bei jeder Attack-Signatur Informationen über die Herkunft, die Schadensbilanz sowie die betroffenen Systeme aus.

Beispiel

Attacke ID=0254 (Tippingpoint-Nummer) unterliegt der internationalen CVE-ID: CAN-2001-0712 bzw. der Bugtraq-ID: 3116. CVE ist eine standardisierte Beschreibung über bekannte Sicherheitslücken (**C**ommon **V**ulnerabilities and **E**xposures; vgl. **`http://www.cve.mitre.org`**).

Bugtraq ist vergleichbar mit CVE und stellt eine weitere große Datenbank für Sicherheitslücken dar (vgl. **`http://www.securityfocus.com`**).

Die detailreichen Informationen aus den verschiedenen Datenbanken helfen dem Netzwerkadministrator, die Attacke und deren Wirkung zu verstehen. Das ist allerdings für den Betrieb des IPS keine Pflicht, da das System vollständig autonom arbeitet und auch ohne Verständnis des Administrators seinen „Dienst“ versieht.

Aktionen bei Attacken

Die Reaktion auf eine als positiv erkannte Attacke kann vom Administrator für jede Signatur selbst definiert werden. Allerdings ist es sinnvoll, die Standardeinstellungen von Tippingpoint so zu belassen (use category settings). Zweckmäßig wird es, wenn gefährdete Systeme trotz bekannter Sicherheits-

lükken unbedingt in Betrieb und erreichbar bleiben müssen. Hier würde man z. B. die Aktion von „Block“ auf „Notify“ umstellen.

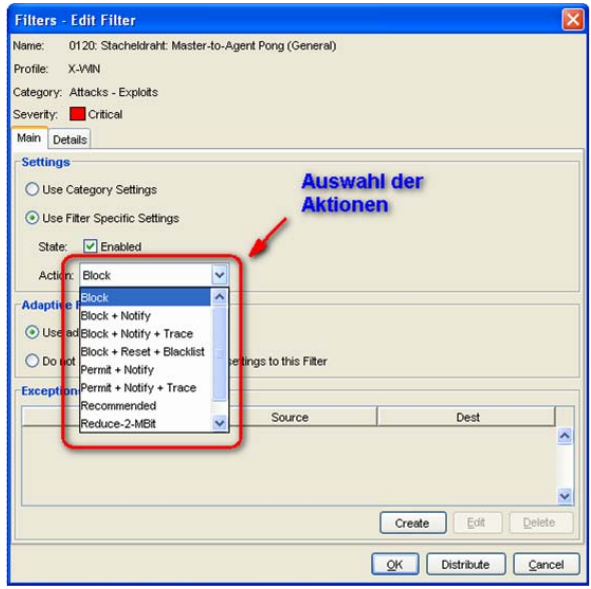


Abb. 5

Überdies kann auch für jeden Filter der Bereich der zu überwachenden IP-Adressen oder -Bereiche als Quelle und/oder Ziel definiert werden. Aber auch hier sollten die Standardeinstellungen genutzt werden.

Arten von Attacken und deren Erkennung im IPS

Viele Attacken benötigen keine Reaktion des vermeintlich betroffenen Systems. Das sind die sog. „SinglePacketAttacks“. Prominentes Beispiel hierfür ist der immer noch sehr verbreitete MS-SQL-Slammer. Hier genügt ein einziges UDP-Paket (Port 1456) auf das Zielsystem. Aufgrund dieser Besonderheit dieser SinglePacketAttacks werden natürlich beliebig viele Zielsysteme schlicht „beschossen“, ohne dass die betroffenen Systeme wirklich verwundbar sind. Diese Art Angriffe gehen wie das „Hornberger Schießen“ aus. Der MS-SQL-Slammer ist auch bei der GWDG die am meisten durch das IPS erkannte und blockierte Attacke und wird aufgrund der Häufigkeit aus unseren Statistiken meist herausgefiltert, da die Anzahl dieser Attacke die anderen Attacken deutlich übersteigt.

Komplexer wird es, wenn auch Antwortpakete des Zielsystems berücksichtigt werden müssen. Deshalb hält das IPS von Tippingpoint bei einer vermeintlichen Attacke mehrere Netzwerkpakete in einem eigenen Speicher, bis der vollständige „Angriffscode“ im IPS vorliegt. Anschließend wird das IPS die Verbindung i. d. R. blockieren. Stellen sich die gesammelten Pakete als „negativ“ heraus, werden diese natürlich an das Ziel weitergeleitet. Dieser Vorgang geschieht natürlich im Bereich von 10^{-6} sec. bis 10^{-3} sec. Das Verfahren ist deshalb wichtig, da sonst ohne eigene „Queue“ bereits Pakete mit schadhaften Code zum Ziel übertragen werden und bei einer Erkennung durch das IPS die meisten Pakete möglicherweise ihr Ziel bereits erreicht haben.

Keine Virenerkennung und dennoch eine Virenabwehr?

Die signaturbasierte Erkennung von Attacken ist nicht zu verwechseln mit der Erkennung von Viren und Trojanern. Wenngleich auch hier Signaturen verwendet werden, bleibt die Erkennung von Viren die zentrale Aufgabe von Virenscannern. Dennoch hat das Tippingpoint IPS die Möglichkeit, die Verbreitung von Viren und Trojanern an einer wesentlichen Stelle zu unterbinden: nämlich im Netzwerk selbst. Nahezu alle Viren müssen sich über bekannte Wege verbreiten (meist via E-Mail oder direkte Netzwerbindungen). Da das IPS die Verfahren für die Ausbreitung vieler Viren als Signaturen kennt, kann bei bereits aktiven Viren die Ausbreitung im Netzwerk durch das IPS erfolgreich verhindert werden. Die derzeitigen Statistiken bei der GWDG auf dem IPS sind sehr ermutigend. Hier erkennen wir an der versuchten Ausbreitung sehr gut, ob bereits im GÖNET betriebene Rechner von Viren oder Trojanern befallen sind.

Erkennen abnormalen Verhaltens

Ein weiteres Verfahren zur Erkennung von Attacken und Angriffen sind die verhaltensbasierten Mechanismen. Hier wird „normales“ von „abnormalem“ Netzwerkverhalten unterschieden. Das IPS hat Ansätze zur Erkennung ungewöhnlicher Aktivitäten im Netz.

Quarantäne

Das IPS bietet die Möglichkeit, durch eine „Quarantäne“-Funktion bestimmte Ereignisse bei Auftreten bestimmter Verhaltensmuster einzuleiten. Wenn z. B. von einer Quell-IP-Adresse mehrfach innerhalb eines definierten Zeitraumes ein Port-Scan ausgeht, kann die Kommunikation der Quell-IP-Adresse mit dem zu schützenden Netz für einen bestimmten Zeitraum „verboten“ werden. Die Quell-IP-Adresse wird so gesehen in „Quarantäne“ geschickt.

Die Auswahl der Ereignisse ist bei Tippingpoint sehr vielfältig und reicht vom

- Blockieren der IP-Adresse auf Zeit,
- Informieren der Administratoren über den Vorfall via E-Mail oder SMS,
- Abschalten von Ethernet-Ports, über die der Angreifer verbunden ist,
- Generieren von Syslog-Einträgen und
- Abschicken von SNMP-Traps

bis hin zur Kombination aus mehreren Ereignissen.

Abb. 6 zeigt einen Auszug aus dem SMS für den Bereich der Quarantäne (Beispiel: Erkennung von NMAP Scans):

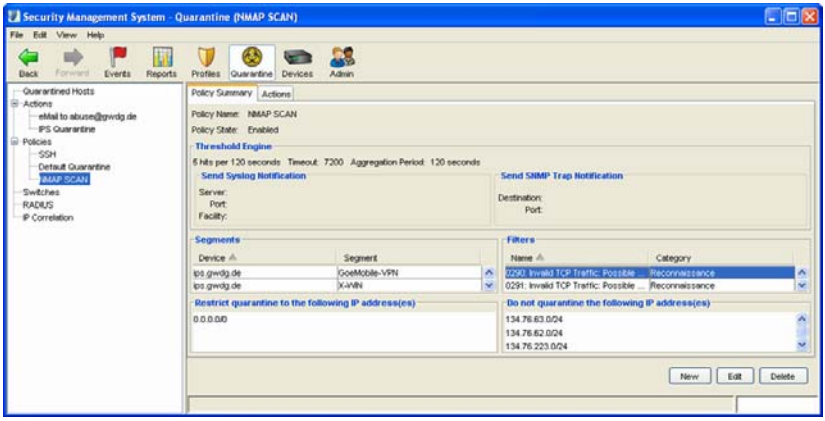


Abb. 6

9.3 Kategorien der Attacken

Im Tippingpoint-IPS wird die „bösartige“ Welt in drei unterschiedliche Kategorien unterteilt, die wiederum jeweils eigene Filter und Untergruppen besitzen (s. Abb. 7):

1. Application Protection
2. Infrastructure Protection
3. Performance Protection

Der Bereich „Performance Protection: Misuse and Abuse“ umfasst im Wesentlichen die Tauschbörsen.

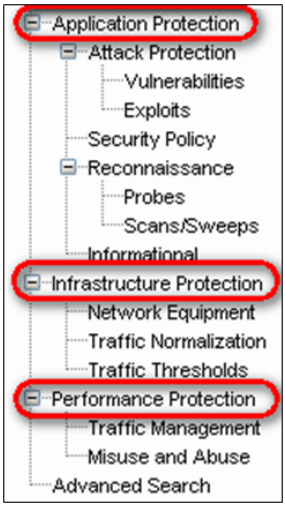


Abb. 7

Unter „Traffic Management“ können Ausnahmen derart definiert werden, dass Quell-IP-Adressen oder -Netze mit Ziel-IP-Adressen/Netze eingerichtet werden (s. Abb. 8), die den gesamten Filtermechanismus des IPS entweder

- umgehen (Trust),
- den Traffic erlauben oder
- oder auf eine definierte Bandbreite begrenzen.

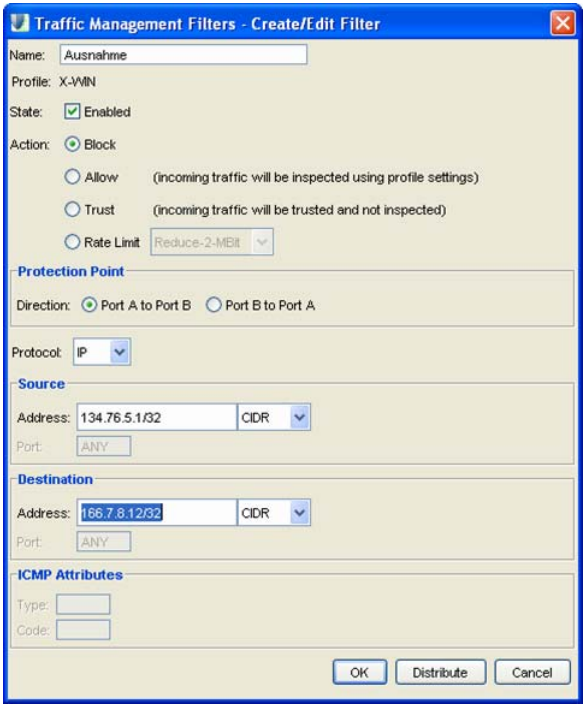


Abb. 8

Diese Einstellungen sind sinnvoll, wenn Netzwerkverkehr trotz verdächtiger Pakete erlaubt werden oder die Bandbreite für bestimmte Systeme begrenzt werden soll.

Im produktiven Betrieb bei der GWDG haben wir Ausnahmen auf dem IPS für unsere FTP-Server eingerichtet, da diese nicht überwacht werden müssen und überdies außerordentlich viel Traffic erzeugen, was lediglich zu einer unnötigen Belastung des IPS führen würde.

Weitere Ausnahmen wurden für spezielle Videokonferenzsysteme innerhalb der Universität Göttingen definiert, welche sehr zeitkritisch sind und dadurch jegliche Verzögerungen im Netzwerk die Bildqualität beeinflussen könnte.

10. Die Testphase bei der GWDG

Im September 2005 hatte die GWDG das IPS Tippingpoint 2004 E unter realen Bedingungen in ihrem Netzwerk im Testbetrieb. Das System wurde

zunächst am Ausgang des Funk-LANs „GoeMobile“ angebunden sowie am Ausgang der Studierendenwohnheime, da hier die höchste Anzahl von möglichen Attacken zu erwarten war. Später wurde das System direkt in den Kommunikationsweg zum Internet mit einer Gesamtbandbreite von 1 GBit/s angebunden.

Ein Schutz der Anbindung zum Internet stellt nicht zuletzt aufgrund der hohen Bandbreite die größte Herausforderung für ein IPS dar. An diesem Übergang zum DFN-Netz bzw. Internet müssen alle Pakete das IPS passieren. Prinzipiell ist dieses auch der ideale Standort für eine zentrale Eindringlingserkennung.

Die folgende Abb. 9 verdeutlicht den Einsatz im Testbetrieb bei der GWDG Ende 2005:

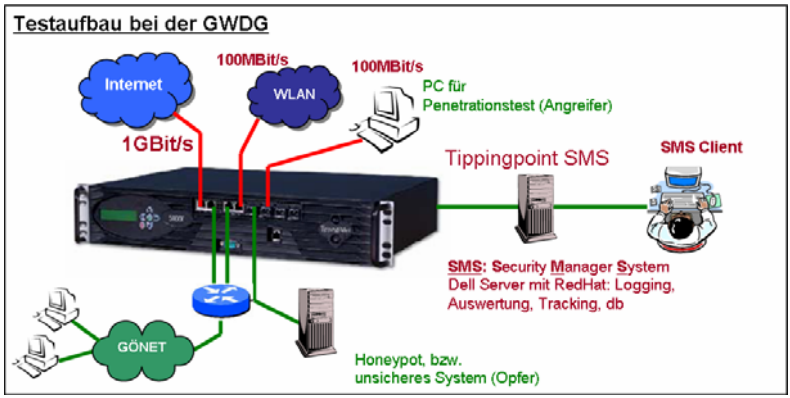


Abb. 9

Am ersten Gigabit-Doppelport wurde das Internet angebunden. Der zweite Doppelport schützt das gesamte Funk-LAN „GoeMobile.“ Am dritten Doppelport wurden für einen Penetrationstest spezielle Systeme angeschlossen. In nahezu unveränderter Konfiguration ist das System derzeit bei der GWDG in Betrieb.

10.1 Test im „GWDG-Lab“ (Penetrationstests)

Das IPS wurde im ersten Schritt einer Reihe von Penetrationstests bei der GWDG unterzogen. Hierbei wurden zwei unterschiedlichen Testszenarien aufgebaut:

1.) Bandbreitentest

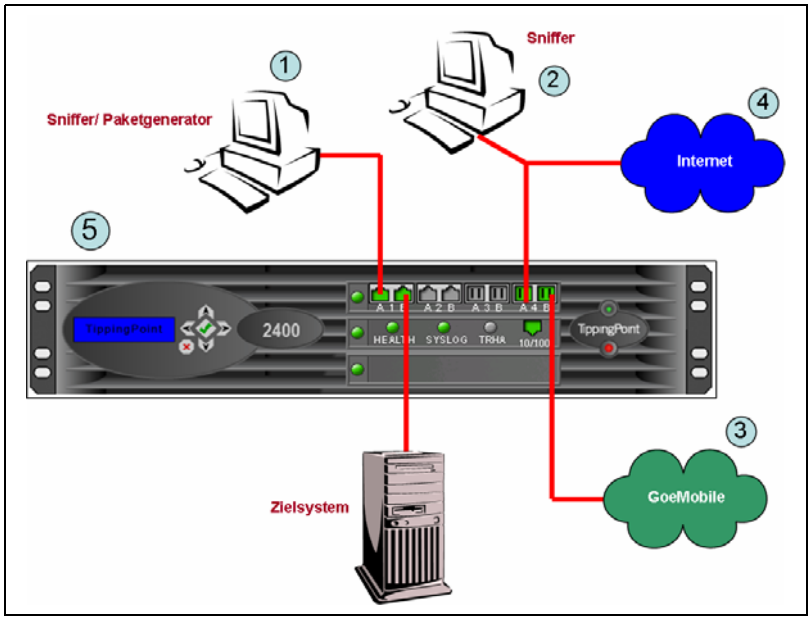


Abb. 10

Mithilfe eines Netzwerksniffers (1), der auch in der Lage ist, eine definierte Netzwerklast zu erzeugen, wurden Pakete bis zu einer Bandbreite von 1 GBit/s generiert. Hierbei wurden UDP- sowie TCP-Pakete beliebiger Auswahl erzeugt. Aber auch UDP-Pakete mit kompromittierendem Inhalt wurden mit Hilfe des Paketgenerators durch das IPS (5) geschickt. Entscheidend für uns war die Reaktion des IPS auf die Netzwerklast in Abhängigkeit der Paketgröße, Anzahl der Pakete pro Sekunde sowie Inhalt und IP-Protokoll. Gleichzeitig wurde auf einem anderen Port-Paar des IPS „normaler“ Netzwerkverkehr durch das IPS geleitet (3) & (4), welcher mit einem weiteren Sniffer (2) am Ausgang des IPS analysiert wurde.

Das Ergebnis war sehr ermutigend. Selbst in der Grenzsituation bei 1 GBit/s an dem Test-Port waren keine Beeinträchtigungen in der Erkennungsleistung auf den anderen Ports des IPS wahrzunehmen. Die Prozessorleistung des IPS stieg erwartungsgemäß an, erreichte aber maximal 65 %. Mit einem weiteren Sniffer am Ausgang des zweiten Port-Paares wurde der „normale“ Traffic beobachtet, während am ersten Port-Paar der Traffic-Generator die künstliche Last erzeugte. Der Netzwerkverkehr wurde auf Paketverluste und Latenzen untersucht. Dabei wurden keine Paketverluste festgestellt. Die Latenzen

stiegen nur in sehr geringem Maße an und lagen im Bereich von 1 bis 2 * 10^{-6} sec.

2.) Penetrationstest: Attacken und illegaler Traffic

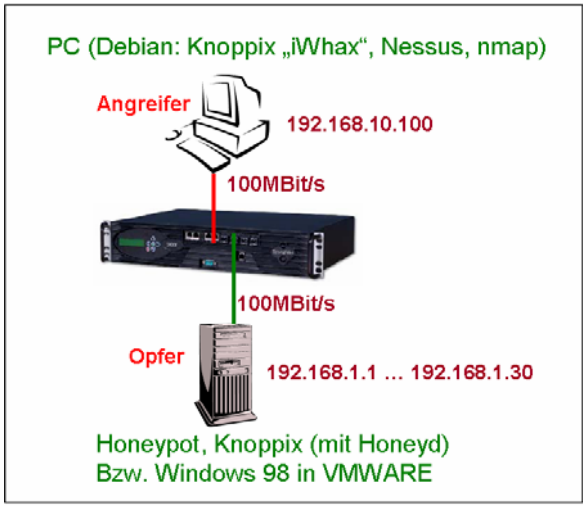


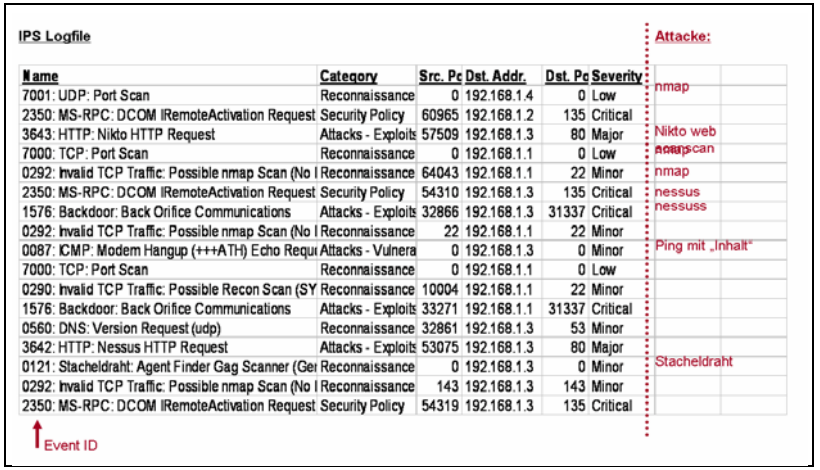
Abb. 11

In einem zweiten Test stand weniger die Bandbreite als vielmehr die Qualität der Erkennung von Attakken durch das IPS im Vordergrund.

Das angreifende System bestand aus einem Linux-System (Debian). Als Portscanner wurde zunächst NMAP verwendet. Weitere Angriffe wurden mit einem von CD bootfähigem Debian-Linux initiiert. Dahinter steht eine speziell für Angriffe produzierte Linux-Version mit dem Namen „iWhax“ bzw. Whoppix. Die CD enthält eine reichhaltige Sammlung von Exploits und weiteren Angriffsprogrammen. Mithilfe dieser CD wurden diverse Attacken auf bekannte Sicherheitslücken gefahren, um die Erkennungsleistung des IPS überprüfen zu können.

Das Ergebnis war sehr zufrieden stellend. Die folgende Abb. 12 zeigt als Ergebnis die Angriffe (linke Spalte) sowie die Erkennung durch das IPS.

Teilweise wurde sogar das Programm, mit dem die Angriffe gestartet wurden, korrekt erkannt (z. B. Nikto WebScan).



IPS Logfile

Name	Category	Src. Pc	Dst. Addr.	Dst. Pc	Severity
7001: UDP: Port Scan	Reconnaissance	0	192.168.1.4	0	Low
2350: MS-RPC: DCOM IRemoteActivation Request	Security Policy	60965	192.168.1.2	135	Critical
3643: HTTP: Nikto HTTP Request	Attacks - Exploits	57509	192.168.1.3	80	Major
7000: TCP: Port Scan	Reconnaissance	0	192.168.1.1	0	Low
0292: Invalid TCP Traffic: Possible nmap Scan (No I	Reconnaissance	64043	192.168.1.1	22	Minor
2350: MS-RPC: DCOM IRemoteActivation Request	Security Policy	54310	192.168.1.3	135	Critical
1576: Backdoor: Back Orifice Communications	Attacks - Exploits	32866	192.168.1.3	31337	Critical
0292: Invalid TCP Traffic: Possible nmap Scan (No I	Reconnaissance	22	192.168.1.1	22	Minor
0087: ICMP: Modem Hangup (+++ATH) Echo Requ	Attacks - Vulnera	0	192.168.1.3	0	Minor
7000: TCP: Port Scan	Reconnaissance	0	192.168.1.1	0	Low
0290: Invalid TCP Traffic: Possible Recon Scan (SY	Reconnaissance	10004	192.168.1.1	22	Minor
1576: Backdoor: Back Orifice Communications	Attacks - Exploits	33271	192.168.1.1	31337	Critical
0560: DNS: Version Request (udp)	Reconnaissance	32861	192.168.1.3	53	Minor
3642: HTTP: Nessus HTTP Request	Attacks - Exploits	53075	192.168.1.3	80	Major
0121: Stacheldraht: Agent Finder Gag Scanner (Ge	Reconnaissance	0	192.168.1.3	0	Minor
0292: Invalid TCP Traffic: Possible nmap Scan (No I	Reconnaissance	143	192.168.1.3	143	Minor
2350: MS-RPC: DCOM IRemoteActivation Request	Security Policy	54319	192.168.1.3	135	Critical

Event ID

Attacke:

nmap

Nikto web

nessus

nessuss

Ping mit „Inhalt“

Stacheldraht

Abb. 12

Honeypot als Opfer-System

Ein Honeypot-System war bei vielen Attacken unser Zielsystem (Opfer). Honeypots simulieren das Verhalten diverser Dienste (Webserver, Mailserver, Telnet-Daemons etc.), ohne jedoch wirklich deren Sicherheitslücken zu besitzen. Überdies werden auch Betriebssysteme simuliert bis hin zu ganzen Netzen von Servern. Ein Honeypot wurde deshalb als Ziel ausgewählt, da es selbst ein Logfile über die Angriffe führt, welches für die Auswertung im Rahmen eines Tests besonders geeignet ist.

Unsicheres Betriebssystem als Opfersystem

Dennoch ist ein Honeypot für einen Angriff auf bekannte Sicherheitslücken nur beschränkt sinnvoll, da es nicht exakt das Verhalten der Sicherheitslücke „simuliert“. Teilweise müssen mehrere Pakete sowie Antwortpakete im Netzwerk ausgetauscht werden, damit eine Attacke stattfindet und überhaupt erst erkannt werden kann. Aus diesem Grund wurde als Zielsystem ein Windows-98-Rechner (ohne Security-Patches) installiert. Hier konnten wir diverse Angriffe starten, die nahezu vollständig vom IPS erkannt und verhindert wurden. Das spiegelt auch eher die Realität in lokalen Netzen wieder.

10.2 Fazit des Testbetriebs im „GWDG-Lab“

Das Ergebnis der verschiedenen Tests mit dem IPS von Tippingpoint war sehr positiv. Die vom Hersteller offerierte Bandbreite konnten wir im Test nachweisen. Wenngleich wir nicht alle Filter des IPS ausprobieren konnten, hatten wir viele Stichproben erfolgreich durchführen können.

10.3 Nicht erkannte Attacke(n)

Einzig die von uns initiierte Attacke via SSH konnte nicht korrekt erkannt werden. Wir hatten versucht, mit diversen Benutzernamen auf ein Zielsystem eine SSH-Sitzung aufzubauen (SSH User Scan). Uns war allerdings schon vor dem Test klar, dass eine Erkennung und Identifizierung von multiplen SSH-Verbindungen als Attacke für das IPS ein „Vabanque-Spiel“ sein muss. Wie unterscheidet man mehrere SSH-Sitzungen auf eine IP-Adresse als Ziel von einer legalen Nutzung eines zentralen SSH-Servers?

Das ist eine Frage, die unser IPS auch nicht wirklich beantworten konnte und folglich die SSH-Sitzungen zum Ziel weiterleitete.

Dennoch hat die nicht korrekt erkannte SSH-Attacke das Gesamtbild kaum trüben können. Das IPS stellte sich mit dem im Test gemessenen Leistungen für den Einsatz im GÖNET als ein sehr geeignetes System heraus. Der produktive Betrieb im GÖNET bestätigte in der Folgezeit unsere Erfahrungen im Test.

11. Erfolgreicher Schutz bei Ausbreitungswellen von Viren

Besonders eindrucksvoll waren für uns die erfolgreiche Abwehr der Ausbreitungswellen von Trojanern und Viren in der Praxis.

Hierzu zwei Beispiele:

Beispiel 1:

Am 28.12.2005 wurde eine Sicherheitslücke „WMF-Lücke“ bekannt:

`http://www.f-secure.com/weblog/archives/archive-122005.html#00000752`

Am gleichen Tag gegen Abend wurde automatisch ein entsprechender Filter von Tippingpoint im Rahmen der Signatur-Updates auf unser IPS geladen. Am folgenden Tag (29.12.2005) wurde vor der Sicherheitslücke im Internet gewarnt. Die Aufregung im Internet hinsichtlich dieser Lücke konnten wir zunächst gar nicht teilen und fanden auch keine Hinweise auf WMF-Attaken innerhalb des GÖNET. Bis uns dann am 29.12.2005 auffiel, dass bereits

seit mehr als 24 Stunden das IPS der GWDG sämtliche WMF-Attacken aus dem Internet erfolgreich herausgefiltert hatte und wir deshalb de facto immun gegen diese Attacke waren. In den weiteren Tagen gab es sehr wenige WMF-Attacken von innen durch „eingeschleppte“ Viren. Dessen Ausbreitung von innen nach außen wurde aber wiederum durch das IPS verhindert. So sind unsere Benutzer hinsichtlich der WMF-Attacken von der Ausbreitungswelle weitgehend verschont geblieben.

Die folgende Abb. 13 zeigt den Anstieg der vom IPS blockierten WMF-Attacken Ende Dezember 2005:

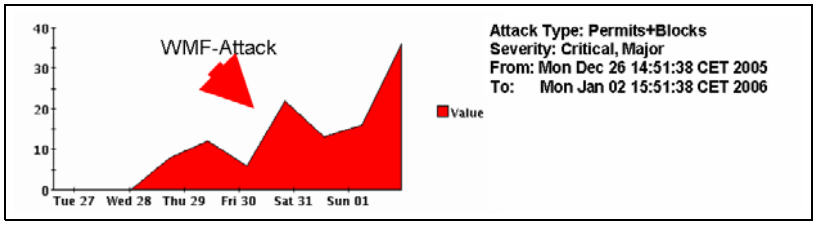


Abb. 13

Beispiel 2:

Am 23.01.2006 wurde vor der „NYXEM.e-Wurm-Ausbreitungswelle“ gewarnt. Am 01.02.2006 hatten wir festgestellt, dass unser IPS bereits einen entsprechenden Filter gegen die Ausbreitung des „NYXEM.e“ geladen hatte. Wir schauten uns die Statistiken an und stellten fest, dass in der Tat alle Mailserver innerhalb des GÖNET das Ziel für die Ausbreitungswelle waren und die Ausbreitung selbst durch das IPS erfolgreich verhindert werden konnte. Da sich „NYXEM.e“ via E-Mail verbreitet, war verständlich, dass ausgerechnet die Mailserver ein primäres Ziel für die Verbreitung darstellten.

Die folgende Tabelle zeigt einen Auszug aus dem Eventlog des IPS bereits wenige Sekunden, nachdem der Filter „aktiv“ wurde*:*

Filter Name	Filter Number	Source IP	Destination IP	Hits	Severity
4122: SMTP: Nyxem.E (CME-24) Worm Email Attachment	4122	x.x.x.x	134.76.10.26	24	Critical
4122: SMTP: Nyxem.E (CME-24) Worm Email Attachment	4122	x.x.x.x	193.175.80.133	11	Critical
4122: SMTP: Nyxem.E (CME-24) Worm Email Attachment	4122	x.x.x.x	134.76.21.104	10	Critical

Abb. 14 zeigt den Anstieg der vom IPS blockierten NYXEM.e-Attacken unmmittelbar nach dem Laden des Filters:

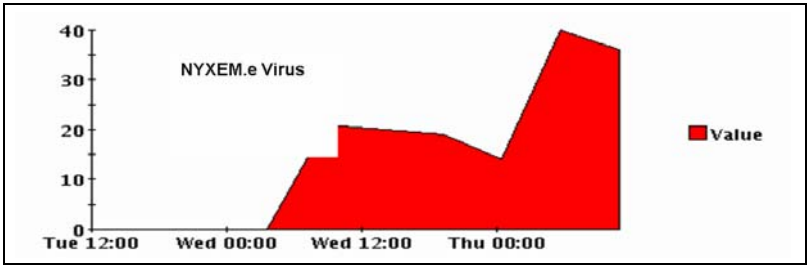


Abb. 14

False Positive Detection

Natürlich ist ein IPS nicht fehlerfrei. Das betrifft auch das Tippingpoint-IPS. Dennoch haben wir im Laborbetrieb sowie auch im produktiven Einsatz lediglich eine einzige nachweisbare False-Positive-Erkennung gehabt. Bei wöchentlich etwa 8 - 9 Millionen Attacken im GÖNET ist das eine sehr akzeptable Leistung.

12. Betrieb im GÖNET

12.1 Auswertungen und Logfiles

Wenngleich das im GÖNET installierte IPS vollständig autonom agiert, ist ein gelegentlicher Blick auf die „Gefährdungslage“ des GÖNET sehr sinnvoll. Das IPS bietet eine große Anzahl an Möglichkeiten, verschiedene Statistiken zu generieren. Da der zum Tippingpoint-System gehörende SMS eine lokale SQL-Datenbank besitzt, in der alle Ereignisse festgehalten werden, können auch im Nachhinein Statistiken über Angriffe und Gefährdungen erzeugt werden.

Über einen Report-Mechanismus können

- Quell-IP-Adressen,
- Ziel-IP-Adressen,
- Zeiten,
- Attacken und
- der Schweregrad der Attacke

für eine Statistik gefiltert und kombiniert werden.

Die folgende Abb. 15 zeigt den ReportManager des Tippingpoint-SMS:

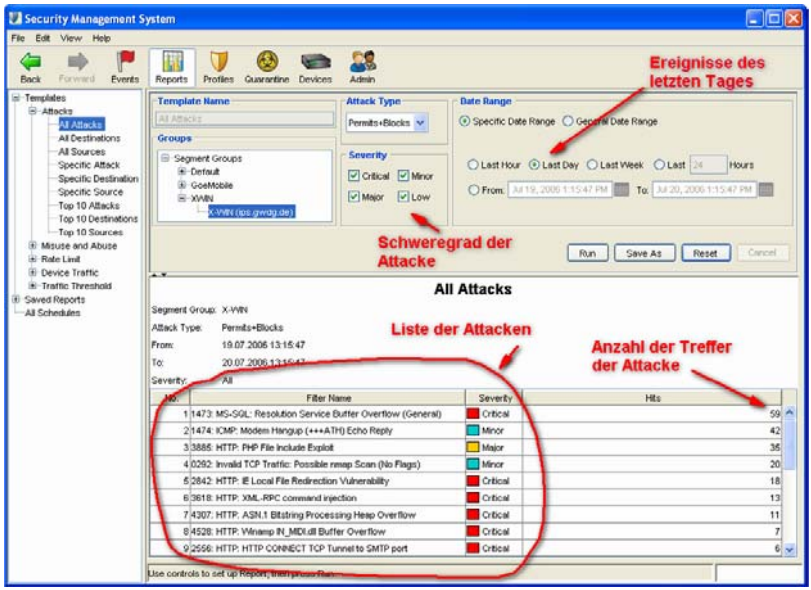


Abb. 15

Überdies sind auch die „TopTen-Angriffe“ über den Report-Mechanismus des SMS verfügbar.

Abb. 16 zeigt als Beispiel die „TopTen“ vom 09.07.2006:

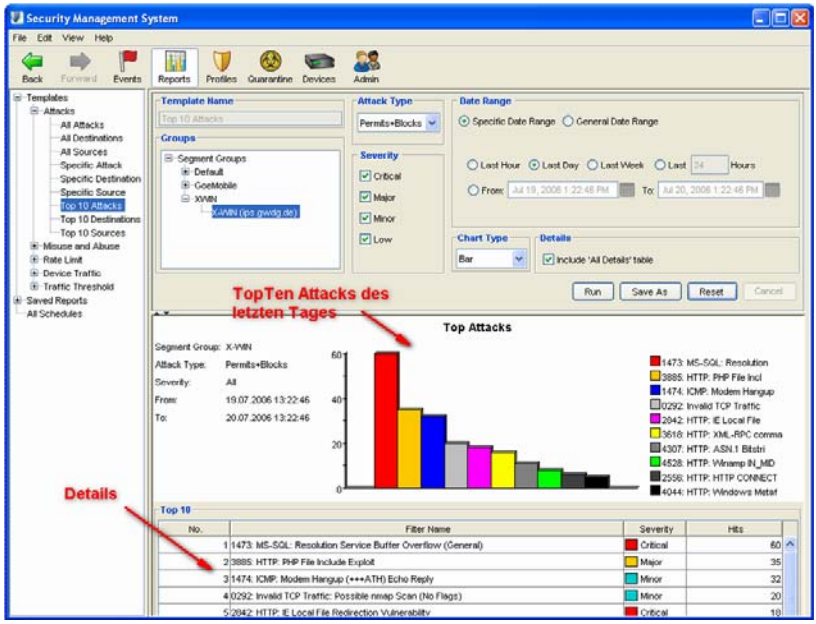


Abb. 16

Das SMS erlaubt auch die zeitgesteuerte Generierung von Statistiken in beliebigen Formaten. Diese können dann entweder per E-Mail verschickt, auf Fileserver kopiert oder via FTP übertragen werden.

Als Formate sind „CSV“, Excel, XML, Bitmap-Bilder oder PDF möglich. Gerade diese Kombinationen lassen kaum noch Wünsche offen.

12.2 Bandbreitenbegrenzung

Neben der Erkennung von Angriffen kann das IPS auch die Bandbreite reduzieren. Gerade im Bereich des „Misuse“ setzen wir diesen Mechanismus erfolgreich ein.

Tauschbörsen

Das IPS erkennt nahezu alle am Markt existierenden Tauschbörsen (derzeit etwa 200 Tauschbörsen). Hierbei werden die Tauschbörsen aber nicht einfach an den bekannten UDP- oder TCP-Ports identifiziert, sondern vielmehr auf hohe Protokollebenen (Layer 7) erkannt. Auch Tauschbörsen, die sich über „well known ports“ wie z. B. Port 80 durchtunneln, werden erfolgreich

identifiziert. Der Tauschbörsenverkehr wird bei der GWDG durch das IPS bewusst nicht blockiert, sondern für alle Tauschbörsen zusammengenommen auf einen Wert von 20 MBit/s limitiert. Auch für das GoeMobile werden Tauschbörsen in der Summe auf einen Wert von 2 MBit/s begrenzt. Tauschbörsen sind also möglich, stören aber aufgrund der Limitierung nicht den anderen Traffic des GÖNET.

Die folgende Abb. 17 zeigt den gesamten Datenverkehr mehrerer Tage, der zum Internet durch das IPS läuft, sowie (unterer dunkler Bereich) alle im GÖNET existierenden Tauschbörsen in der Summe. Hier erkennt man auch deutlich die Bandbreitenlimitierung durch das IPS. Am Tag wird die Grenze von 20 MBit/s erreicht, in der Nacht gehen die Werte deutlich herunter, sodass die Limitierung nicht greifen muss.

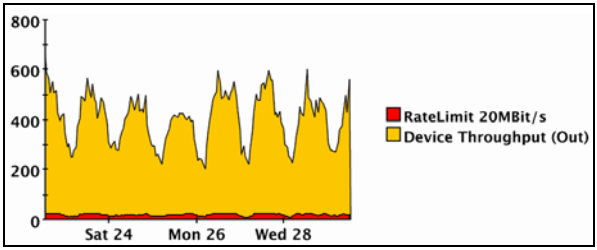


Abb. 17

Ähnlich sieht das Bild auch im GoeMobile aus, allerdings aufgrund der geringeren Bandbreite der Interfaces dann mit entsprechend geringerer Grenze (2 MBit/s).

Durch Bandbreitenbegrenzung für bestimmte Dienste kann das IPS sicherstellen, dass andere wichtige Anwendungen nicht durch Fehlnutzung in deren Funktion beeinträchtigt werden.

12.3 Überwachung des IPS

Das IPS selbst besitzt eine ganze Reihe von Überwachungsmechanismen, um die korrekte Funktion zu gewährleisten. Werden z. B. mehr als 1 % aller Pakete vom IPS aufgrund von ungeklärten Problemen nicht übertragen, schaltet das IPS selbständig in einen sog. Layer-2-Fallback zurück. Das bedeutet, dass die Erkennung des IPS in diesem extrem seltenen und kritischen Fall ausgesetzt wird und die Anschlüsse des IPS einfach durchgeschaltet werden.

Überschreitet die CPU-Belastung des IPS bei der sehr rechenintesiven Analyse der Pakete eine gewisse Schwelle, so werden zunächst alle Logging-

Mechanismen ausgesetzt, um die CPU zu entlasten. Dieses Ereignis ist bei uns in dem neunmonatigen Betrieb bislang dreimal aufgetreten. Das System hatte dann selbstständig das Logging nach wenigen Minuten wieder aktiviert, sobald die Belastung für das System gesunken war. Ursache dafür waren neben dem ohnehin hohen Traffic-Aufkommen des gesamten GÖNET auch die Belastung durch die FTP-Server der GWDG. Immer dann, wenn neue Linux-Distributionen herauskamen, wurde der FTP-Server der GWDG außerordentlich start frequentiert. Wir haben in der Folge die FTP-Server der GWDG im IPS aus der Überwachung herausgenommen.

Monitoring

Ein bei der GWDG eingesetztes Monitoringsystem (CACTI) überwacht, neben vielen anderen Netzkomponenten, auch die Aktivitäten des IPS.

Es ist für jeden Benutzer unter

`http://monitor.gwdg.de`

erreichbar (Bereich: Intrusion Prevention System).

Abb. 18 stellt die CPU-Belastung des GWDG-IPS über eine Woche dar:

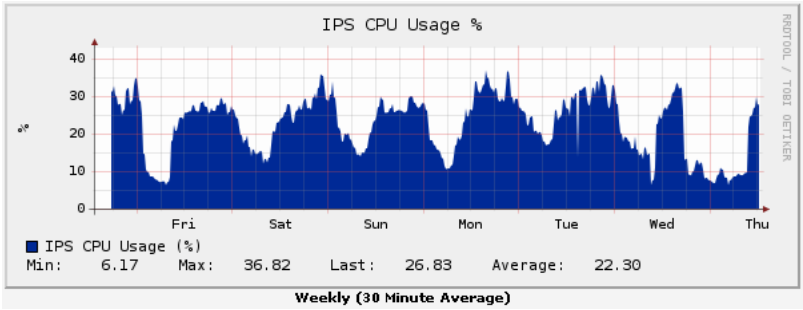


Abb. 18

Dort wird u. a. auch die CPU-Belastung via SNMP aufgezeichnet. Aber auch die Netzwerklast an den Interfaces sowie die „TopTen-Attacken“ werden im CACTI dargestellt.

12.4 Angriffe und Statistiken im GÖNET

Die Angriffe vom Internet in das GÖNET sind vielfältig. Die folgenden Bilder illustrieren den typischen Alltag eines IPS bei der Abwehr von Attacken im GÖNET.

Abb. 19 zeigt die „TopTen-Angriffe“ eines Tages sortiert nach Quell-IP-Adressen:

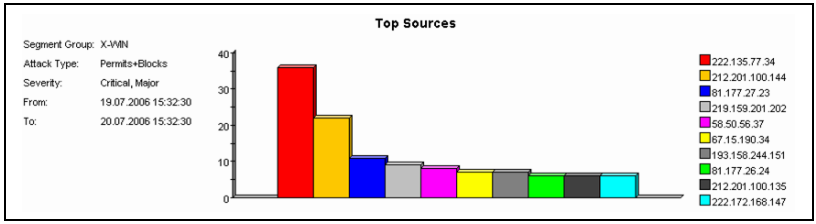


Abb. 19

Abb. 20 stellt die „TopTen-Attacken“ des gleichen Tages sortiert nach Art der Attacke sowie Häufigkeit dar:

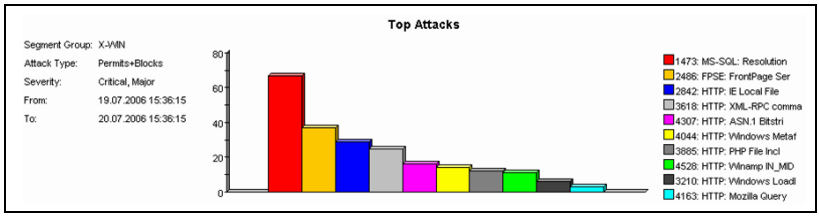


Abb. 20

Abb. 21 verdeutlicht die Anzahl der Angriffe in einer (typischen) Woche:

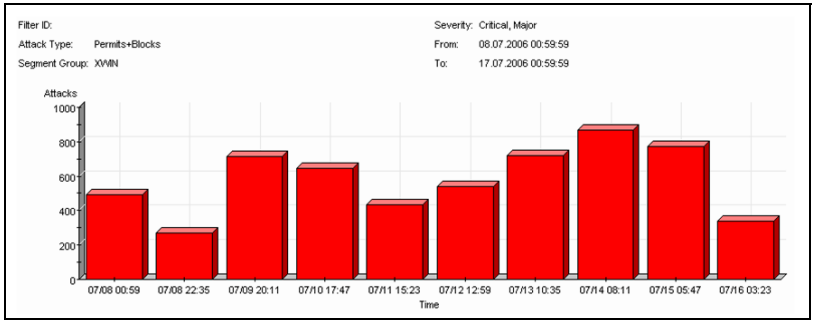


Abb. 21

Täglich werden etwa 1.000 - 2.000 Angriffe in das GÖNET blockiert. In der Statistik wird dabei nicht der MS-SQL-Slammer berücksichtigt, da er in der Summe alle anderen Attacken überdecken würde.

Die folgende Tabelle zeigt die Attacken eines Tages sortiert nach der Art der Attacke:

No.	Filter Name	Severity	Hits
1	3885: HTTP: PHP File Include Exploit	Major	2.326
2	4307: HTTP: ASN.1 Bitstring Processing Heap Overflow	Critical	421
3	1473: MS-SQL: Resolution Service Buffer Overflow (General)	Critical	340
4	2842: HTTP: IE Local File Redirection Vulnerability	Critical	299
5	2486: FPSE: FrontPage Server Extensions Chunked Transfer Overflow	Critical	290
6	2289: MS-RPC: DCOM ISystemActivator Overflow	Critical	207
7	2556: HTTP: HTTP CONNECT TCP Tunnel to SMTP port	Critical	193
8	4193: SMB: ASN.1 Bitstring Processing Heap Overflow	Critical	180
9	1279: HTTP: Shell Command Execution (winnt/system32/cmd.exe)	Critical	158
10	4044: HTTP: Windows Metafile (WMF) Vulnerable Function	Critical	137
11	0238: HTTP: Nimda Attack	Critical	115
12	3979: HTTP: Illegal ActiveX Object Instantiation	Critical	104
13	4163: HTTP: Mozilla QueryInterface() Heap Buffer Overflow	Critical	65
14	3642: HTTP: Nessus HTTP Request	Major	61
15	0495: HTTP: Shell Command Execution (cmd.exe)	Major	60
16	3273: HTTP: AWStats Multiple Vulnerabilities	Critical	48
17	3618: HTTP: XML-RPC command injection	Critical	40

13. Derzeitiger Betrieb

Das IPS ist derzeit fast unverändert so in Betrieb, wie es im Rahmen der ersten Tests installiert wurde. Mittlerweile gab es natürlich eine Reihe von Firmware-Updates des Herstellers, die einige Features hinzugefügt haben.

Das IPS besitzt vier transparente Gigabit-Doppelports, von denen ein Portpaar für die Absicherung des gesamten GÖNET dient. Hier ist direkt das DFN/Internet-Netz mit einer Bandbreite von 1 GBit/s über das IPS mit dem GÖNET verbunden.

Das zweite Portpaar sichert die Kommunikation direkt hinter unserem zentralen VPN-Gateway ab. Das VPN-Gateway wird hauptsächlich vom GoeMobile benutzt und bedarf einer getrennten Absicherung.

Abb. 22 illustriert den Einsatz des IPS im Netz der GWDG (Stand: 7/2006):

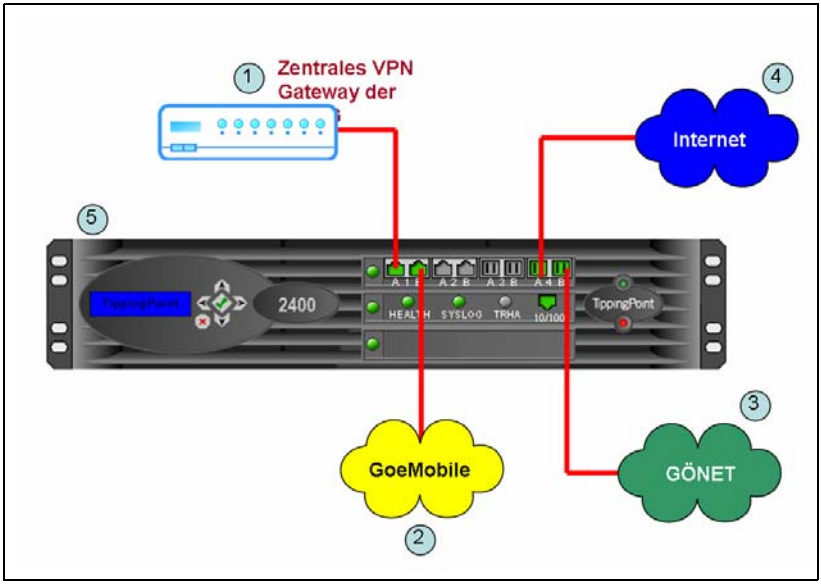


Abb. 22

Die anderen beiden freien Portpaare werden in den kommenden Monaten in Betrieb genommen und bestimmte Servernetze absichern, sodass auch Attacken, die nicht aus dem Internet kommen, die Server nicht gefährden können.

14. Ausblick

In Zukunft werden wir die ausführlichen Loggingmechanismen des SMS nutzen, um die Benutzer im GÖNET frühzeitig auf eine mögliche Infektion des eigenen Rechners hinweisen zu können. Wir sammeln jetzt bereits die Angriffsalarmierungen des IPS in einer eigenen SQL-Datenbank. Uns interessieren hier vor allem die Attacken von innen nach außen, da in diesem Fall ein Rechner im eigenen Netz bereits befallen ist. Da die IP-Adresse des Rechners sowie die Art, Zeitpunkt und die Häufigkeit der Attacke festgehalten werden, können wir ein befallenes System einem Institut zuordnen. Unser späteres Ziel ist es, den dort tätigen Systemadministrator dann automatisch via E-Mail über die kompromittierten Rechner zu informieren.

15. Fazit

Das IPS in der GWDG stellt einen idealen und dringend erforderlichen Baustein zur Sicherung des lokalen Netzwerkes dar. Es ersetzt natürlich keine Firewall, kann aber gerade in Kombination mit einer Firewall einen sehr hohen Schutz bieten. Eine Firewall allein ist nicht in der Lage, diesen vielen Arten teilweise sehr subtiler Angriffsmuster adäquat begegnen zu können. Momentan können wir in dieser Kombination einen ausgereiften Gesamtschutz für unsere Institute und deren Benutzer zur Verfügung stellen.

Die Statistiken und vor allem die schnelle automatisierte Reaktion auf Ausbreitungswellen von Viren zeigen, dass mit dem IPS eine wesentliche Lücke zwischen Virenschutz und Firewall geschlossen werden konnte. Damit einher geht auch ein Gewinn an Arbeitszeit, die ansonsten aufgrund erfolgreicher Attacken mit der daraus folgenden „Wiederbelebung“ der infizierten Rechner verloren gehen würde.

Portknocking – Zugang erst nach Anklopfen

Marcello Bellini

Max-Planck-Institut für ausländisches und internationales Strafrecht, Freiburg

Einleitung

Als Administrator sucht man immer neue Wege, um seine Server vor Angriffen zu schützen. Eine zur Zeit immer weiter verbreitete Methode ist das so genannte Portknocking.

Bei Portknocking handelt es sich um eine zusätzliche Möglichkeit, um Dienste auf einen Server zu sichern. Der Dienst erst bei Bedarf in der Firewall freigeschaltet.

1. Wie funktioniert Portknocking?

Auf dem Server laufen eine Firewall, unter Linux üblicherweise iptables, diverse Serverdienste und der so genannte Portknocking-Server. Nehmen wir einmal an, dass wir einen ssh-Zugang für Wartungszwecke benötigen. Dieser Dienst muss nicht ständig über das Internet verfügbar sein und kann

somit erstmal in der Firewall gesperrt werden. Dadurch ist der Dienst von außen nicht erreichbar und somit auch nicht angreifbar (s. Abb.1).

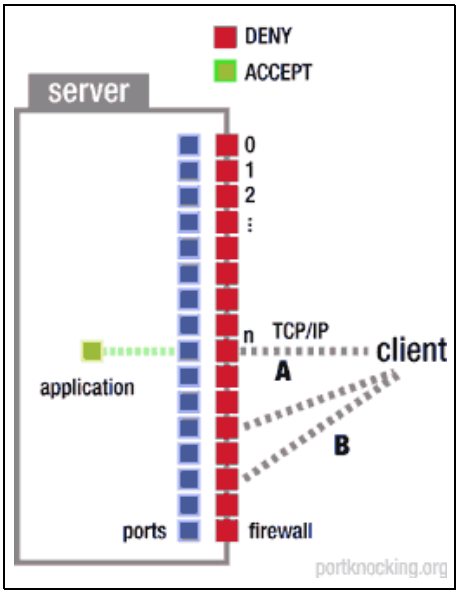


Abb. 1

Damit nun aber ein Client eine Verbindung zu dem ssh-Server aufbauen kann, muss zunächst der Port in der Firewall freigeschaltet werden, in unserem Beispiel Port 22. An diesem Punkt kommt der Portknocking-Server (PK-Server) ins Spiel. Der PK-Server „lauscht“ an der Firewall auf eine festgelegte Paketfolge, wenn diese erkannt wird, schaltet der PK-Server den ssh-Port in der Firwall frei. Meist wird der Port sogar nur für die IP-Adresse des klopfenden Rechners freigeschaltet (s. Abb. 2 u. 3).

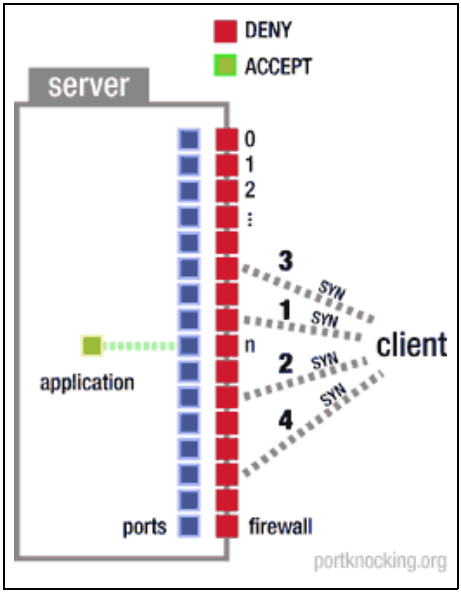

DENY
ACCEPT
server
0
1
2
3
1
n
2
4
SYN
SYN
SYN
SYN
client
application
ports
firewall
portknocking.org

Abb. 2

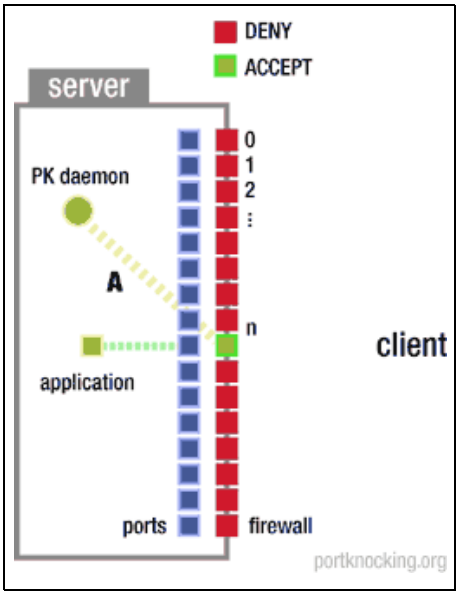

DENY
ACCEPT
server
PK daemon
A
0
1
2
n
client
application
ports
firewall
portknocking.org

Abb. 3

Nun kann sich der Client ganz normal an dem ssh-Server anmelden (s. Abb. 4). Es gibt bei den meisten PK-Servern die Möglichkeit eine Zeitbegrenzung anzugeben, wie lange der Port in der Firewall freigeschaltet bleiben soll. Bereits bestehende Verbindungen sind von dieser Zeitbegrenzung nicht betroffen. Dadurch wird verhindert, dass, während der Client mit dem Server verbunden ist, weitere Verbindungen aufgebaut werden können.

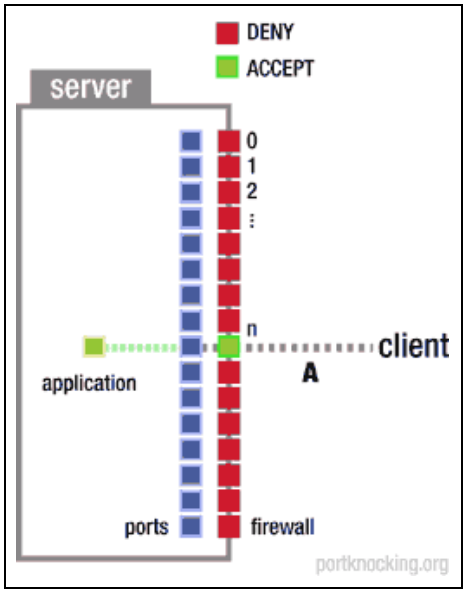


Abb. 4

2. Wieso Portknocking?

Mitte 2004 erhöhte sich die Anzahl der „Brute-Force“-Angriffe auf ssh-Server. Dies war kein vereinzeltes Problem, sondern wurde weltweit beobachtet (http://isc.sans.org/diary.php?date=2004-07-23):

```
Jul 14 02:12:19 rage sshd[47297]: Illegal user admin from
203.197.118.71
Jul 14 02:12:25 rage sshd[47299]: Illegal user test from
203.197.118.71
Jul 14 02:12:30 rage sshd[47301]: Illegal user guest from
203.197.118.71
Jul 14 02:12:37 rage sshd[47303]: Illegal user webmaster from
203.197.118.71
Jul 14 02:12:41 rage sshd[47305]: Illegal user mysql from
203.197.118.71
Jul 14 02:12:45 rage sshd[47307]: Illegal user oracle from
203.197.118.71
Jul 14 02:12:50 rage sshd[47309]: Illegal user library from
203.197.118.71
Jul 14 02:12:54 rage sshd[47311]: Illegal user info from
203.197.118.71
Jul 14 02:12:59 rage sshd[47313]: Illegal user shell from
203.197.118.71
```

Wie man sieht, handelt es sich hier um automatisierte Versuche, einen validen Benutzeraccount auf dem Server zu finden.

Nach dieser Angriffswelle folgte dann die nächste Stufe, bei der dann für die gefunden Benutzer verschiedene Angriffe entweder mit Wörterbuchattacken oder tatsächlich gesammelten Passwörtern versucht wurde. Bei der Menge der Angriffe und der verwendeten Passwörter bestand die reelle Gefahr, dass tatsächlich ein gültiges Passwort gefunden wird.

3. Welche Vorteile bringt Portknocking?

Wenn der Dienst nicht erreichbar ist, kann er – selbst wenn eine Schwachstelle vorhanden ist – nicht kompromittiert werden. Dadurch hat man sogar einen effektiven Schutz gegen so genannte „Zero-Day“-Exploits, die Schwachstellen ausnutzen, welche noch nicht öffentlich bekannt sind und für die es somit auch noch keinen Patch gibt.

4. Was gibt es für Lösungen?

Seit den Anfängen von Portknocking (1999) haben sich verschiedene Lösungen für unterschiedliche Anforderungen entwickelt. Es gibt auch so exotische Lösungen wie DNS-Knocking oder HTTP-Knocking (http://

www.webknocking.de), welche nicht mehr, wie der ursprüngliche Ansatz an einem geschlossen Port klopft, sondern bereits einen offenen Port für die Kommunikation mit dem Portknocking-Dienst verwendet. Ein guter Schutz gegen das Abhören der Klopf-Sequenz lässt sich durch verschiedene Zusatzfunktionen - um ein Höchstmaß an Sicherheit zu erzielen - erreichen. Angefangen bei einer HTTPS-Anfrage (beim HTTP-Knocking), Einmal-Sequenzen bis hin zu Verschlüsselung der Klopf-Sequenz.

5. Portknocker

Eine gute Quelle für Informationen über Portknocking ist die Seite http:www.portknocking.org. Hier sind zur Zeit 30 verschiedene Portknocker aufgelistet, zu diesen gehört alles von „proof-of-concept“-Lösungen aus Hacker-Kreisen bis hin zu ausgereiften Lösungen für den Produktiveinsatz. Leider sind einige Links zu Projekten nicht mehr aktuell und funktionieren nicht mehr. Im Folgenden sollen einige der interessantesten Lösungen kurz vorstellt werden.:

cd00r

Dieses Programm wird als „proof-of-concept“-Lösung vorgestellt. cd00r ist eines der ersten bekannten Portknocker-Programmen. Solche Lösungen wurden gerne in Hackerkreisen für die Einbindung von backdoors in gekaperte Systeme verwendet. Diese waren von außen nicht sichtbar und konnten trotzdem noch Zugang zu den Systemen gewähren.

webknocking (http://webknocking.de)

Hierbei handelt es sich um eine Lösung, die meiner Meinung nach eine gute Lösung für einen Webserver wäre, da hier der Server auf einem bereits offenen Port lauscht und die Klopf-Sequenz aus der HTTP-Anfrage ausliest.

wknock (http://www.rstack.org/oudot/wknock/)

Dieses Projekt versteckt ganze Access-Points, um es „War-Drivern“ schwer zu machen, diese Netze zu entdecken bzw. zu nutzen. Dazu sind aber spezielle Access-Points nötig, die mit der OpenWRT-Firmware (http://www.openwrt.org) laufen.

winportknocking

Eine der wenigen Lösungen, die Windows als Server-System unterstützen. Winportknocking benötigt die kommerzielle CHX-1-Firewall für Windows (http://www.windows-firewall.com).

6. Ein Beispiel aus der Praxis

Ein relative einfach zu implementierendes Beispiel ist der knockd (http://www.zeroflux.org/knock). Für die meisten Linux-Distributionen gibt es bereits fertige Pakete. Man muss dazu eine Firewall (z. B. iptables) und den knockd–Dämon auf dem Server installieren. Beide Pakete sind bei den meisten Linux-Distributionen schon enthalten. Danach müssen nur noch wenige Schritte unternommen werden, um den Dienst in Betrieb zu nehmen. Als erstes muss man die Konfigurationsdatei anpassen; diese liegt standardmäßig unter /etc/kockd.conf oder /etc/knockd/knockd.conf.

```
[options]
logfile = /var/log/knockd.log
interface = eth0

[opencloseSSH]
one_time_sequences = /etc/knockd/ssh_sequences
seq_timeout = 15
start_command = /usr/sbin/iptables -A input -s %IP%
-p tcp --dport 22 -j ACCEPT
cmd_timeout= 60
stop_command= /usr/sbin/iptables -D INPUT -s %IP%
-p tcp --dport 22 -j ACCEPT
```

Wenn man von der Möglichkeit der „Einmal-Sequenzen“ Gebrauch macht, muss man noch eine Datei anlegen und mit festgelegten Sequenzen befüllen. Diese Sequenzen sind folgendermaßen aufgebaut: Eine Sequenz pro Zeile (jede Sequenz sollte mit einem Leerzeichen beginnen, da benutzte Sequenzen mit einem „#“ auskommentiert werden), die Ports sind durch Kommata getrennt und können, wenn nicht nur TCP-Pakete verwendet werden, nach dem Port mit einem Doppelpunkt vom Protokoll getrennt werden. Beispielweise könnte eine solche Sequenzdatei folgendermaßen aussehen:

```
1234:TCP,2222:UDP,5432:UDP,2000:TCP
2345,3333,1025,3333,4321
```

Bei der ersten Zeile handelt es sich um eine gemischte Sequenz aus TCP und UDP Paketen, während in der zweiten Zeile nur TCP-Pakete erwartet werden.

Client

Der Client wird auch gleich mitgeliefert und lässt sich über den Befehl knock aufrufen. Um sich beispielsweise über die erste Sequenz zu verbinden, genügt der Aufruf:

```
knock server.mpicc.de 1234:TCP 2222:UDP 5432:UDP
2000:TCP
```

Nachdem der Server die Sequenz erkannt hat, wird das start_command-Ereignis ausgelöst. In diesem Fall wird in der Firewall die IP-Adresse des klopfenden Clients auf Port 22 freigeschaltet. Jetzt kann sich der Client ganz normal zu dem ssh-Server verbinden. Dies muss aber in unserem Beispiel innerhalb von 60 Sekunden geschehen (cmd_timeout=60), danach wird der stop_command ausgeführt und Port in der Firewall wieder geschlossen. Bestehende Verbindungen werden dabei nicht abgebrochen.

7. Fazit

Portknocking ist eine gute Möglichkeit, die Sicherheit von Systemen zu erhöhen. Portknocking eignet sich natürlich nicht für Systeme, auf die sich auch „normale“ Benutzer einloggen sollen, da es noch keine komfortablen Client-Programme gibt, die von jedem Benutzer bedient werden können. Es bietet aber einen guten Schutz für z. B. ssh-Zugänge, die eigentlich nur für Wartungs- bzw. Administrationszwecke verwendet werden.

Quellen:

Abbildungen: http://en.wikipedia.org/wiki/Port_knocking

Portknocking, In: Hackin9 6/2005

Horch, wer kommt von draußen rein, In: ct' 14/2004

Portknocking (URL: http://www.datenterrorist.de/portknocking)

Links:

http://www.portknocking.org

http://www.netfilters.org

http://www.openbsd.org/faq/pf/

Das Compute-Grid der GWDG

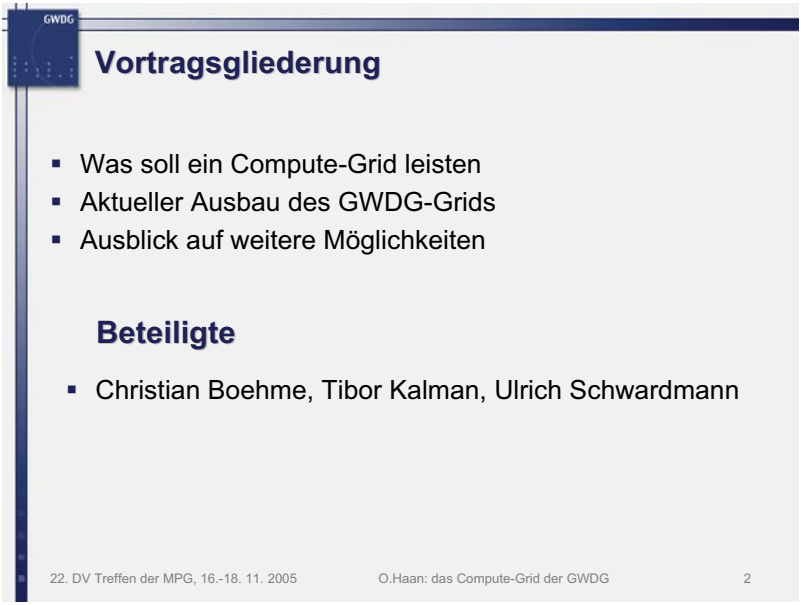
Oswald Haan

Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

1. Einleitung

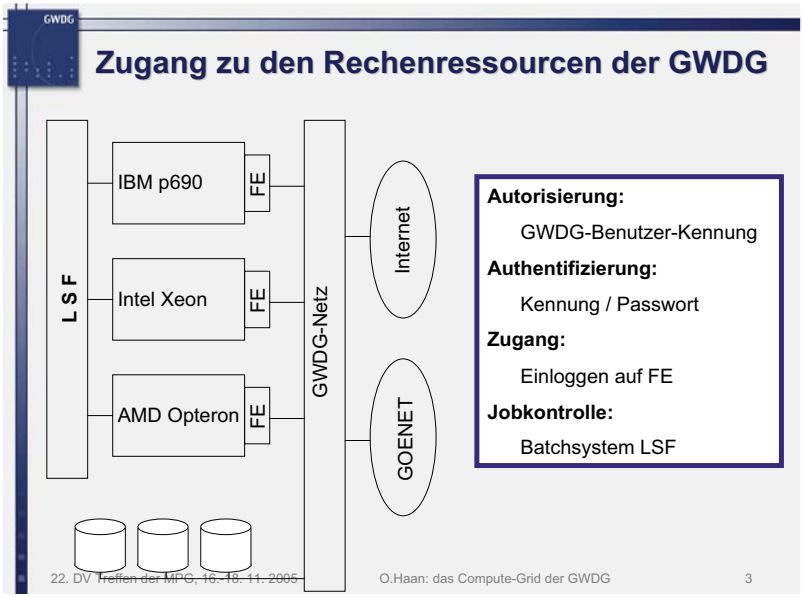
Die Grid-Technologie hat zum Ziel, Rechenleistung, Speicherplatz, Daten und Anwendungen auf transparente Weise zur Verfügung zu stellen. In Analogie zum Stromnetz (daher der Name Grid) sollen IT-Leistungen an jedem Ort auf gleiche Weise nutzbar sein, ohne dass sich der Nutzer um die dafür notwendige Infrastruktur zu kümmern hätte. Er soll nur für den Abschluss vertraglicher Regelungen zur Abnahme der Leistungen zuständig sein.

An der hierfür notwendigen Infrastruktur wird seit einigen Jahren weltweit intensiv gearbeitet. Die Standardisierung von Leistungen und von Schnittstellen ist inzwischen so weit fortgeschritten, dass die wissenschaftlichen Rechenzentren Grid-Technologien zur Nutzung ihrer Ressourcen einsetzen können. Dieses Ziel verfolgt die GWDG mit dem Aufbau eines Compute-Grids. Den Inhalt des Berichtes über dieses Projekt gibt die folgende Folie:



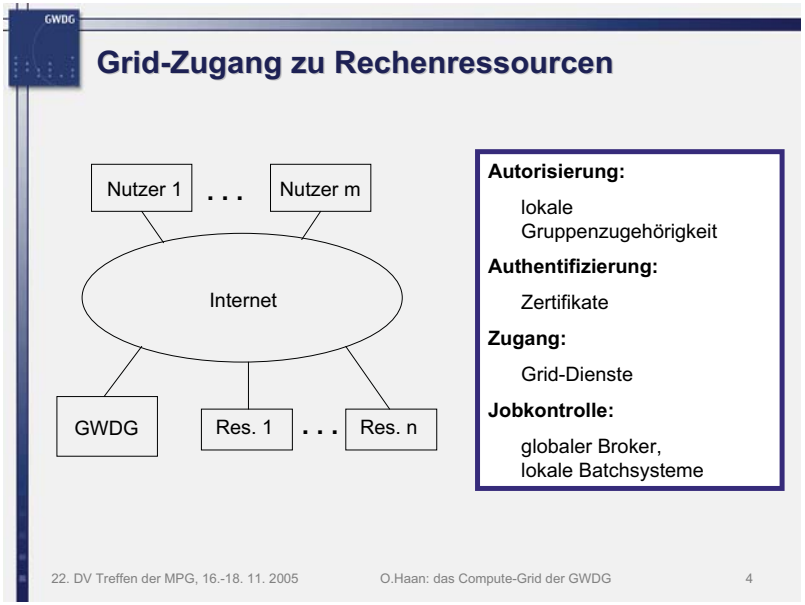
2. Was soll ein Compute-Grid leisten?

Zur Beantwortung dieser Frage sei zunächst der herkömmliche Weg zur Bereitstellung der Rechenleistung aufgezeigt:

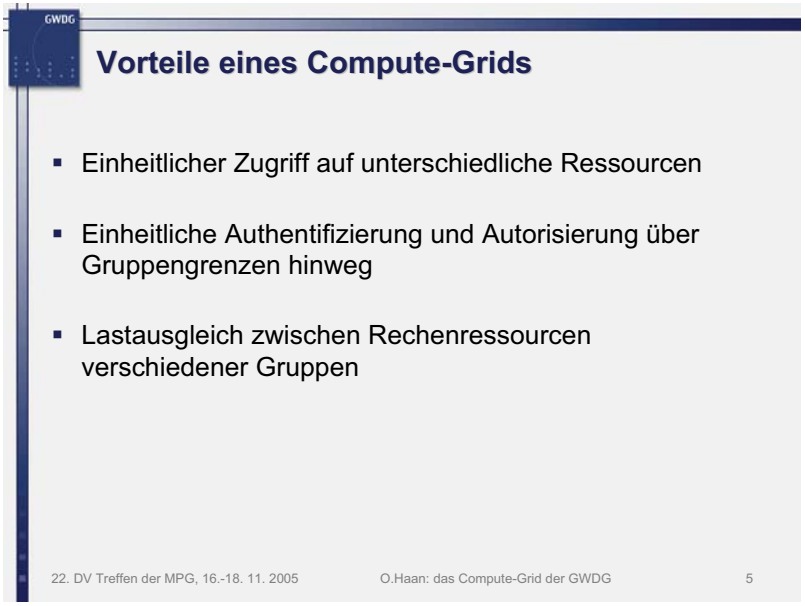


Das charakteristische Merkmal dieser Zugriffsweise ist, dass Nutzer in der lokalen Nutzerverwaltung geführt werden müssen, sich mit dem nur lokal gültigen Passwort authentifizieren müssen und auf dem lokalen Rechner zur Bearbeitung von Aufgaben Jobs in das lokale Batch-System einbringen müssen. Sollen Ressourcen eines anderen Rechenzentrums eingesetzt werden, muss der Nutzer sich mit der dort vorhandenen Umgebung auseinandersetzen.

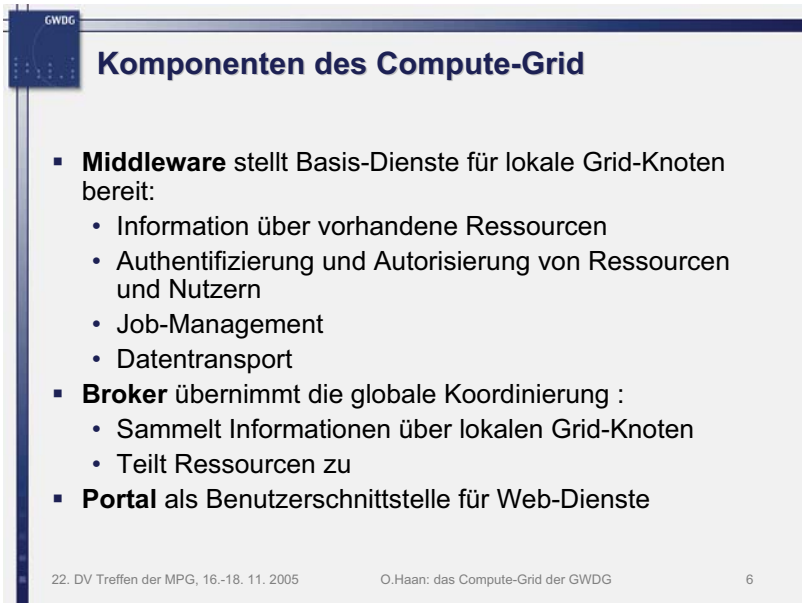
Mit der Verfügbarkeit eines Grids sollten verschiedene lokale Ressourcen für den Nutzer erreichbar sein, ohne dass er sich auf die lokalen Eigenheiten der Ressourcen einstellen muss.



Die Autorisierungsfrage wird durch Zugehörigkeit zu Gruppen geregelt, die auf den lokalen Ressourcen Nutzungsberechtigung haben. Die Authentifizierung erfolgt durch global gültige Zertifikate. Die Leistungen werden als standardisierte Dienste über einen Browser im Internet nachgefragt. Die Auswahl der Ressourcen, die die Leistungen erbringen, erfolgt über einen Broker, dem lokale Grid-Knoten ihre Ressourcen anbieten.

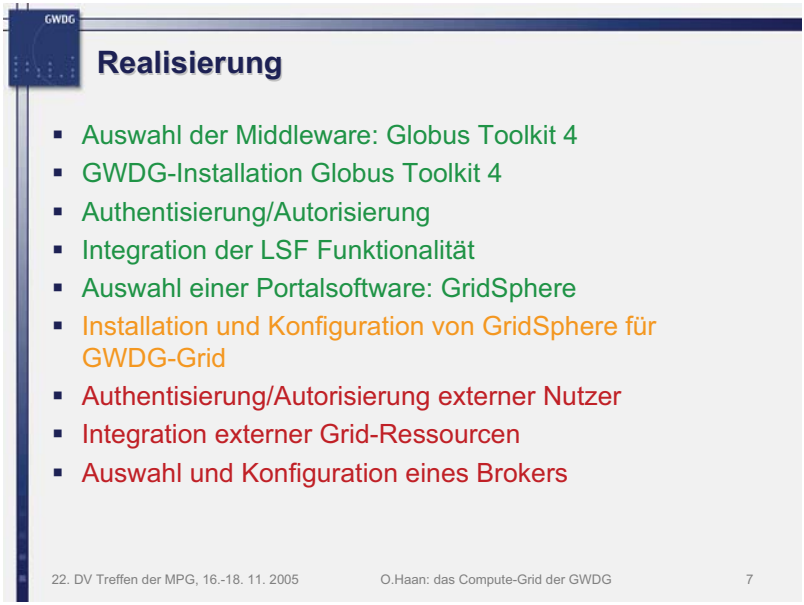


Im Einzelnen müssen die folgenden Komponenten zur Realisierung eines Grids bereitgestellt werden:

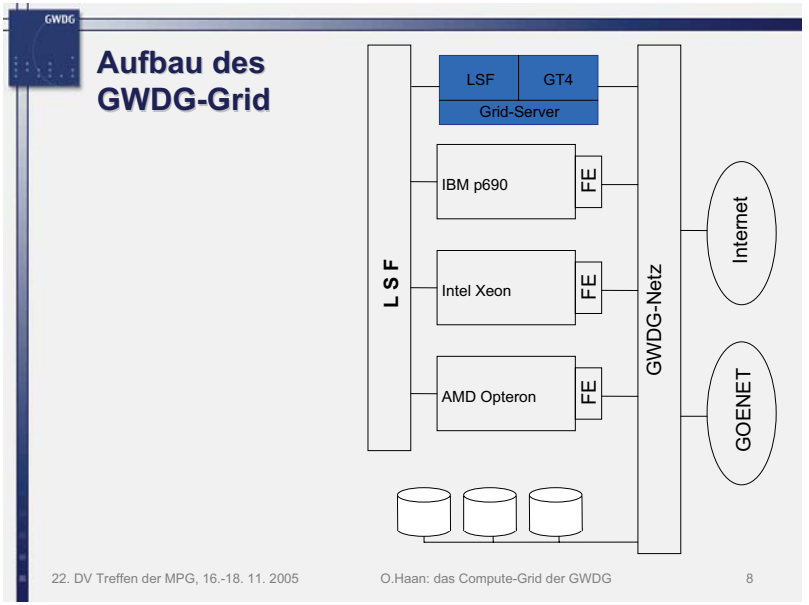


3. Aktueller Ausbau des GWDG-Grids

Die folgende Folie zeigt die Arbeitschritte, die zum Aufbau des Compute-Grids der GWDG durchzuführen sind:

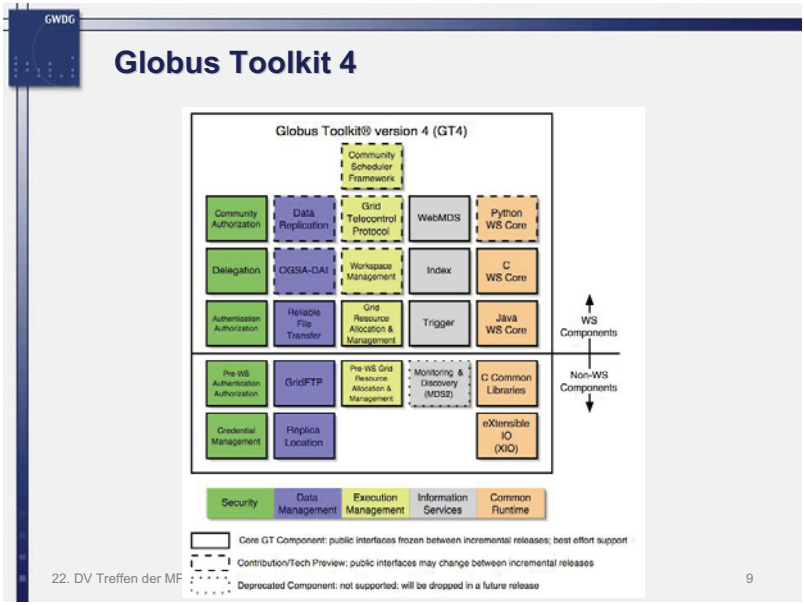


Die ersten fünf Aufgaben sind bereits erledigt und sollen nun kurz beschrieben werden. Das Grundkonzept ist in der folgenden Folie dargestellt:



Auf einem Grid-Server wird als Middleware das Produkt Globus Toolkit 4 bereitgestellt. Globus Toolkit ist eine frei verfügbare und in vielen Grid-Projekten erprobte Software. Insbesondere wird Gobus Toolkit (GT) auch im D-Grid-Projekt eingesetzt. Auf dem gleichen Server steht die Schnittstelle zum lokalen Batch-System LSF zur Verfügung, so dass Aufgaben, die über das Grid gestartet werden, dem Batch-System übergeben werden können.

Globus Toolkit 4 enthält die folgenden Komponeneten für ein Grid:



Die Security Komponente ist für Authentifizierung und Autorisierung zuständig. Bei der GWDG wurde diese Komponente so konfiguriert, dass zum einen Zertifikate der in GT integrierten Zertifizierungsstelle Simple CA akzeptiert werden, zum andern die von der GWDG-CA erzeugten Grid-Zertifikate gültig sind. Die Simple-CA-Zertifikate werden nur in der Test-Phase des GWDG-Grids genutzt, in einem späteren Produktionsbetrieb werden die Zertifikate der GWDG-CA oder einer übergeordneten CA verlangt werden. Die Autorisierung erfordert zurzeit noch eine GWDG-Kennung, da nur damit eine Nutzung der Batch-Ressourcen der GWDG erlaubt ist. Diese Autorisierung wird durch die Zuordnung von Zertifikaten zu gültigen Benutzerkennungen in der Datei grid-mapfile von GT erreicht.

Authentifizierung und Autorisierung mit GT4

- Authentisierung
  - Zertifikate nach dem Standard X.509
  - Nutzer und Ressourcen werden zertifiziert
  - Delegation von Zertifikaten: Single Sign On
  - Erlaubte Zertifizierungs-Stellen:
    Simple CA, GWDG CA
- Autorisierung
  - GWDG-Kennung nötig für Nutzung der LSF-Ressourcen
  - Zuordnung Zertifikat – Kennung:
    grid-mapfile in GT4

GT definiert Dienste zum Job Management, wie in den folgenden drei Folien beschrieben:

Job Management in GT4
GRAM : Grid Ressource Allocation & Management

- Jobs abschicken:
  `globusrun-ws -submit -job-command /bin/hostname`
- weitere Optionen:
  `-factory <localhost | http://gwdg-wk01.gwdg.de:8080/wsrf/services /ManagedJobFactoryService | ...>`

  `-factory-type <fork | LSF | ...>`

  `-job-epr-output-file <job.epr>`

  `-job-description-file <job.desc>`
- Jobs verwalten
  `globusrun-ws -status -job-epr-file <job.epr>`
  `globusrun-ws -kill -job-epr-file <job.epr>`

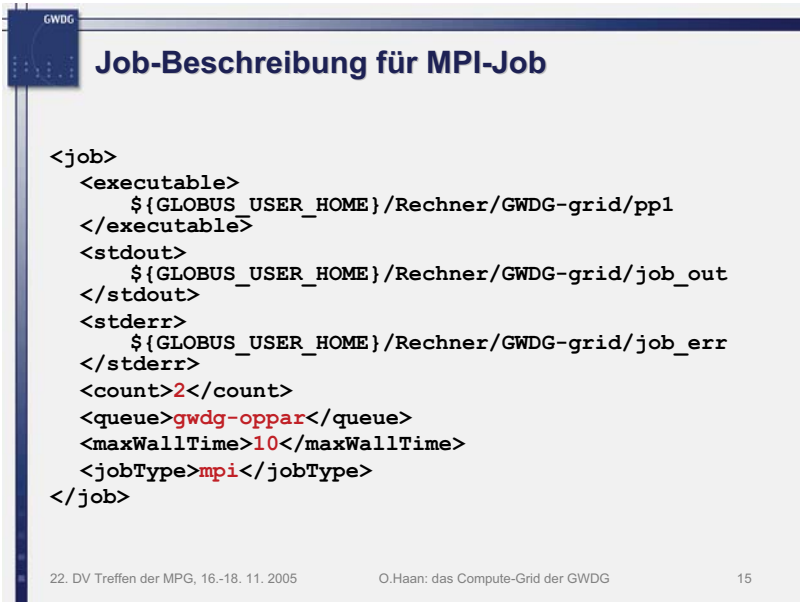
Job Description File

- XML Syntax
- Elemente:
  - Queue
  - jobType (single, multiple, mpi)
  - count
  - hostCount
  - maxWallTime
  - maxMemory
- Transfer von Ein- und Ausgabedateien

Beispiel Job Description

```
<job>
    <executable>my_echo</executable>
    <directory>${GLOBUS_USER_HOME}</directory>
    <argument>Hello world!</argument>
    <stdout>${GLOBUS_USER_HOME}/stdout</stdout>
    <stderr>${GLOBUS_USER_HOME}/stderr</stderr>
    <fileStageIn>
        <transfer>
            <sourceUrl>gsiftp://submit.host:2888/bin/echo</sourceUrl>
            <destinationUrl>file:///${GLOBUS_USER_HOME}/my_echo</destinationUrl>
        </transfer>
    </fileStageIn>
    <fileStageOut>
        <transfer>
            <sourceUrl>file://${GLOBUS_USER_HOME}/stdout</sourceUrl>
            <destinationUrl>gsiftp://submit.host:2888/tmp/stdout</destinationUrl>
        </transfer>
    </fileStageOut>
    <fileCleanUp>
        <deletion> <file>file://${GLOBUS_USER_HOME}/my_echo</file> </deletion>
    </fileCleanUp>
</job>
```

Diese Dienste werden auf die entsprechenden Funktionen des lokalen Batch-Systems LSF abgebildet:



Von GT4 erzeugtes LSF-Jobfile

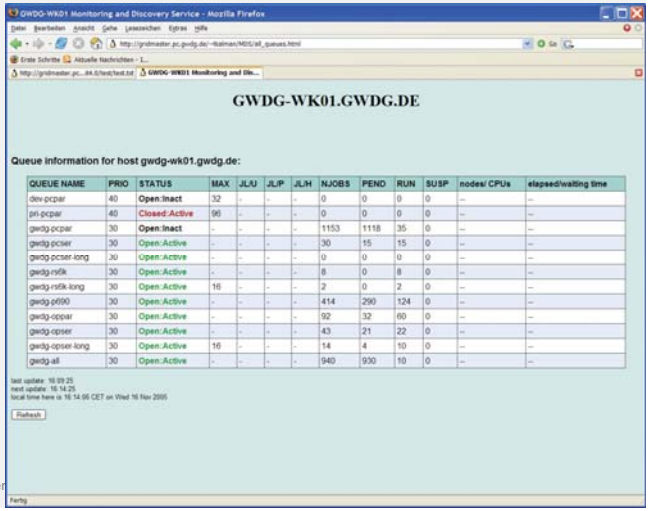
```
#! /bin/sh
#
# LSF batch job script built by Globus Job Manager
#
### test line
### Globus::GRAM::JobDescription=HASH(0x827f63c):
###2;
#BSUB -q gwdg-oppar
#BSUB -W 10
#BSUB -i /dev/null
#BSUB -o /usr/users/ohaan/Rechner/GWDG-grid/g_out
#BSUB -e /usr/users/ohaan/Rechner/GWDG-grid/g_err
#BSUB -n 2
...
#Change to directory requested by user
cd /usr/users/ohaan
. /opt/hplsf/conf/profile.lsf && mpirun.globus
        /usr/users/ohaan/Rechner/GWDG-grid/pp1
```


Informationen über laufende und wartende Jobs werden von GT aus den entsprechenden LSF-Kommandos ausgelesen und mit den Monitory & Discovery Services von GT bereitgestellt:

GT4 Informationsdienste MDS2

- MDS2 speichert Informationen in LDAP
- Informationen können mit LDAP Anfragen abgerufen werden
- Ergebnisse der LSF-Kommandos bqueues werden im GWDG-Grid bereitgestellt

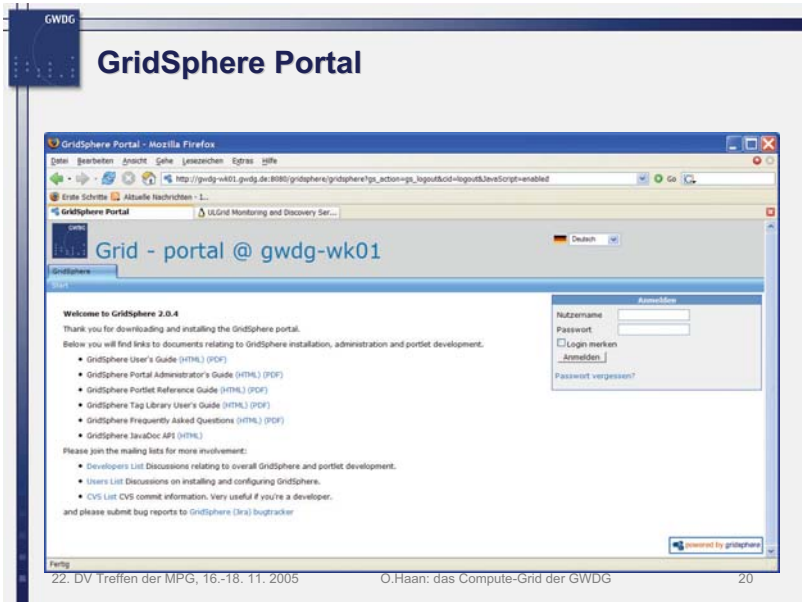
Queue-Informationen über MDS2



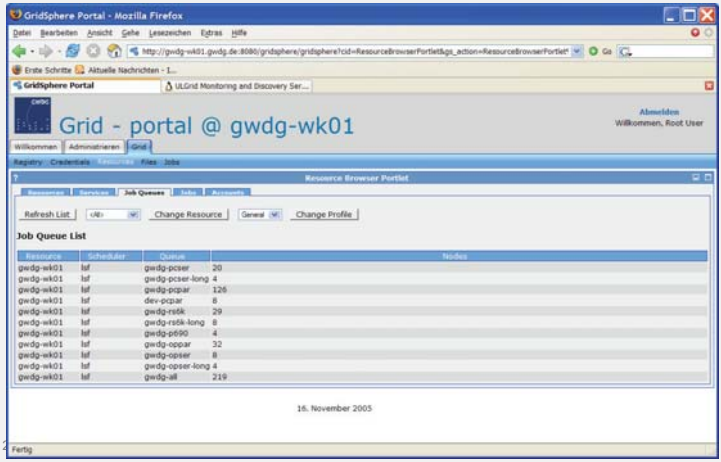
GT4 Informationsdienste MDS4

- MDS2 wird in kommenden Versionen nicht mehr unterstützt
- MDS4 basiert auf XPath anstatt auf LDAP
- LSF-Informationen noch nicht über MDS4 verfügbar

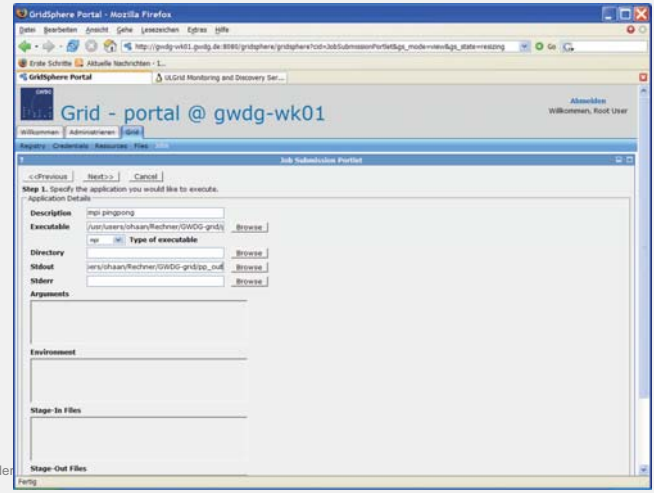
Einen einfacheren Zugang zu den Grid-Diensten von GT bietet ein Web-Portal, das über einen beliebigen Browser angesprochen werden kann. Im Compute-Grid der GWDG ist die Portal-Software GridSphere eingebunden. Die folgenden Folien zeigen Beispiele für die Nutzung von Grid-Diensten über dieses Portal:



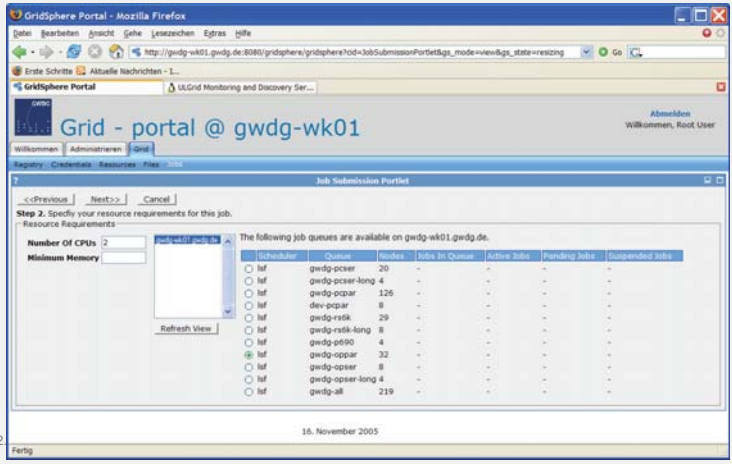
Statische Queue-Informationen



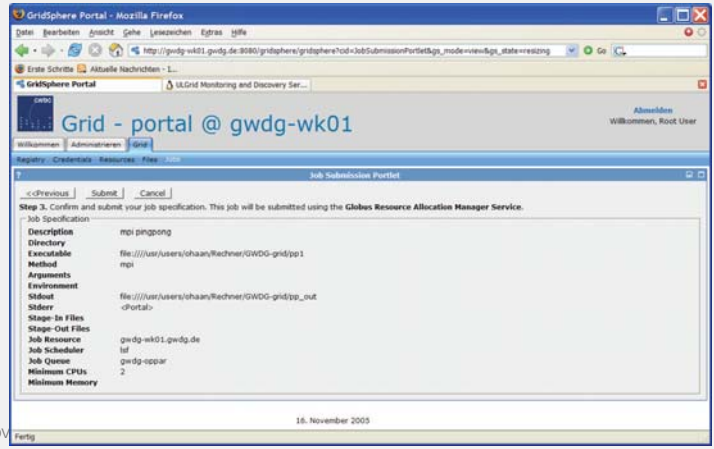
Job abschicken



Job abschicken

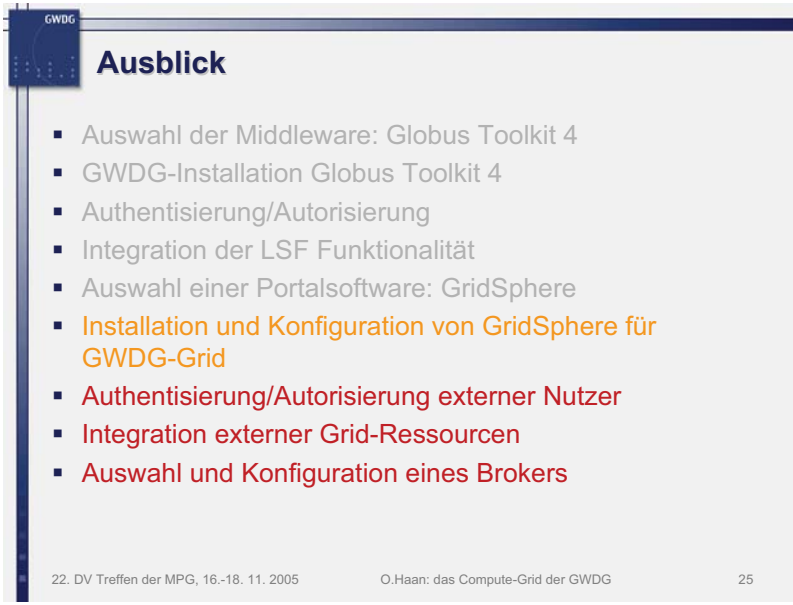


Job abschicken



4. Ausblick

Die Grundfunktionalität zur Nutzung der Batch-Ressourcen über eine Grid-Schnittstelle ist damit im Compute-Grid der GWDG realisiert. Allerdings erlauben diese bisher nur eine lokale Nutzung. Die Vorteile des Grids werden den Nutzern erst dann zugute kommen, wenn die Einbindung externer Nutzer und externer Ressourcen verwirklicht ist und ein Broker bereitsteht, der für jeden Auftrag aus der Menge aller eingebundenen Ressourcen die am besten geeignete zuweist.



Das Instant-Grid – ein Grid-Demonstrations-Toolkit

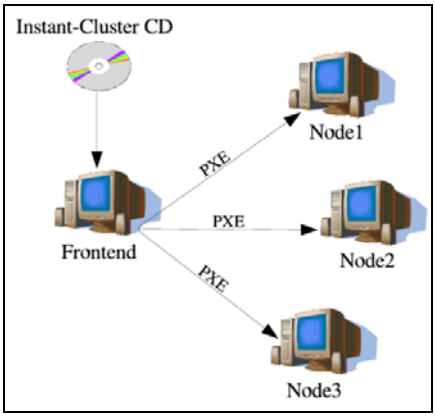
Christian Boehme

Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

1. Das Konzept des Instant-Grids

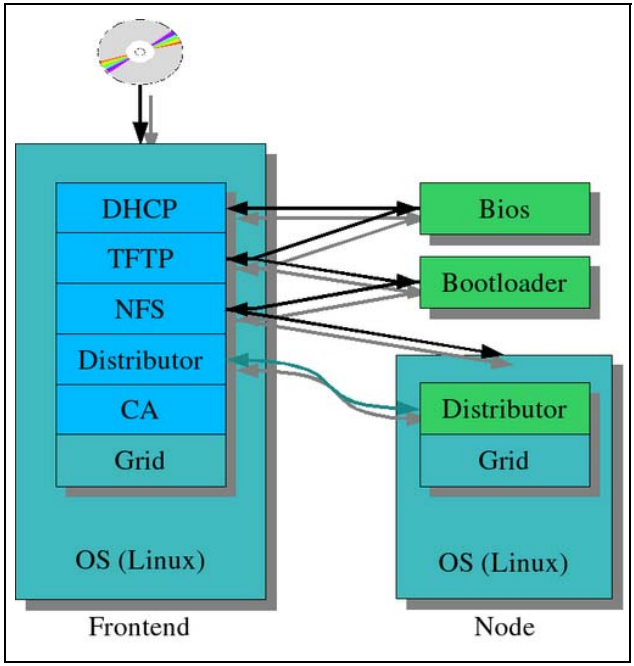
1.1 Das Funktionsprinzip

Übersicht



Das „Instant-Grid" soll einen einfachen Zugang zu Grid-Technologien ermöglichen. Es handelt sich um eine mit minimalen Aufwand zu installierende, weitestgehend vorkonfigurierte Grid-Umgebung in Form eines PC-Clusters, der von einer CD-ROM bzw. per PXE(Pre-Execution Boot-Environment)-Boot gestartet wird. Die vorhandene Umgebung wird dabei nicht dauerhaft verändert, so dass beliebig zwischen Grid-fähigem Linux-Cluster und originaler Konfiguration gewechselt werden kann.

Der Startvorgang



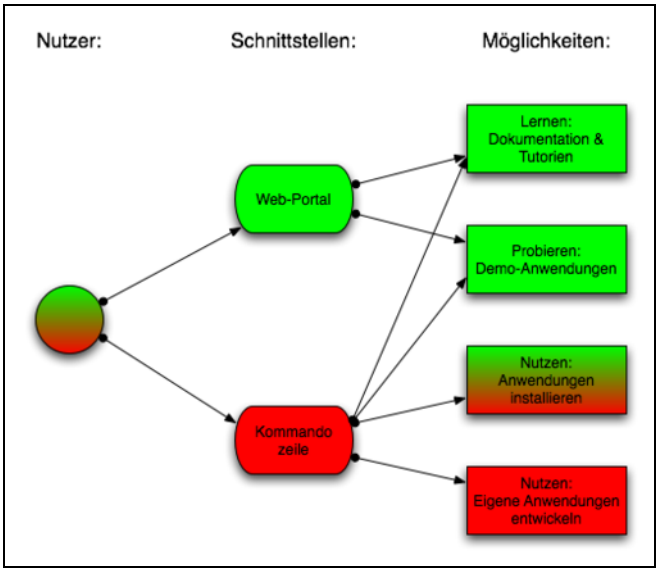
Gestartet wird zunächst ein Terminalserver. Unter diesem Begriff sind verschiedene Server zusammengefasst, die auf dem Grid-Frontend vorkonfiguriert von der CD-ROM gestartet werden, um im Folgenden weiteren Rechnern (Clients) den Start und die Integration in das lokale Grid per PXE-Boot zu erlauben. Dazu gehören vor allem ein DHCP-Server für die Zuteilung der IP-Nummern und die Bekanntgabe der PXE-Boot-Informationen, ein TFTP-Server, auf dem ein Bootloader, Kernelimage und Miniroot für die Clients bereitgehalten werden und ein NFS-Server, von dem die Clients das eigentliche Root-Verzeichnis (auf der CD-ROM enthalten) sowie eventuell Datenaustauschverzeichnisse einhängen können. Ferner läuft hier der DISTRIBUTORD für das automatische Kopieren aktualisierter Konfigurations-

dateien und die automatische Bearbeitung von Host-Zertifizierungsanfragen sowie der IPCOLLECTOR für die automatische An- und Abmeldung neuer bzw. aus dem Grid entfernter Clients.

Nach dem Terminalserver können die Clients gestartet werden. Entsprechend der vom DHCP-Server des Terminalservers erhaltenen Informationen laden die Clients den PXELINUX-Bootloader vom TFTP-Server. PXELINUX lädt dann Kernelimage und Miniroot vom TFTP-Server, die dann die CD-ROM per NFS als Rootfilesystem einhängen. Dann starten die Clients den DISTRIBUTORCD. Zu seinen Aufgaben gehört das Einhängen der vom Frontend exportierten Verzeichnisse und das Erstellen der für jeden Client notwendigen Host-Zertifizierungsanfrage.

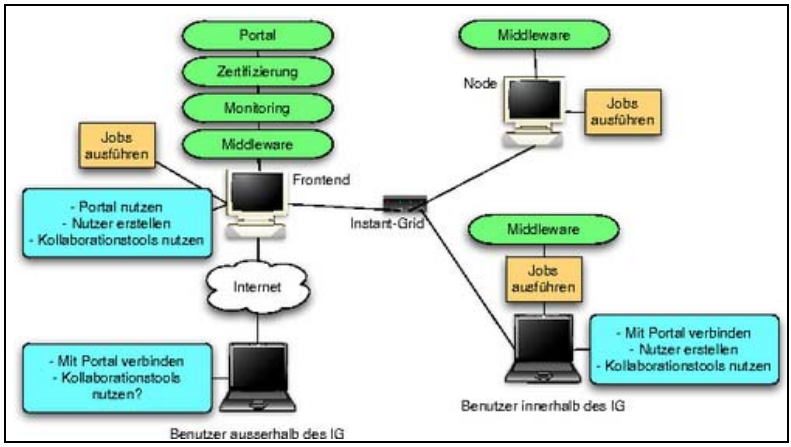
1.2 Nutzungsmöglichkeiten

Nutzerzentrierte Sicht



In der obigen Grafik werden die Zugangsmöglichkeiten zum Instant-Grid und die darüber erreichbare Funktionalität dargestellt. Die für Anfänger bezüglich Grid-Software vorgesehenen Zugänge bzw. Nutzungsmöglichkeiten sind etwas heller dargestellt als diejenigen für Nutzer mit Vorkenntnissen. Über das einfach zu bedienende Portal können die Tutorien und die Dokumentation verwendet und die mitgelieferten Demonstrationsanwendungen bedient werden. Erfahrenen Nutzern stehen Kommandozeilen-Tools zur Verfügung, über die die volle Grid-Funktionalität verfügbar ist.

Rechnerzentrierte Sicht



Die Bedienung des Instant-Grids erfolgt immer über den Frontend-Knoten. Bei Verwendung des Portals ist es weitgehend gleichgültig, ob von innerhalb oder außerhalb auf den Frontend zugegriffen wird. Die Erstellung von Portal-Nutzern steht aus Sicherheitsgründen allerdings nur Clients innerhalb des Instant-Grid zur Verfügung. Natürlich können auch nur Instant-Grid-Clients Grid-Jobs ausführen.

2. Status

2.1 Was ist auf der CD enthalten?

Das Instant-Grid befindet sich zur Zeit in der Entwicklung, eine Version 1.0 ist für den Spätherbst 2006 geplant. Bereits jetzt können aber Vorab-Versionen getestet werden. Die Vorab-Version vom November 2005 basiert auf einem im Umfang reduzierten Knoppix 4.0.2. Als Grid-Middleware kommt das Globus Toolkit 4.0 zum Einsatz, ergänzt durch Globus MPI für das Ausführen MPI-parallelisierter Programme.

2.2 Was funktioniert bereits?

Im November 2005 standen folgende Funktionen zur Verfügung:

- Automatisches Setup des Clusters
  - Automatisches Setup des Netzwerkes
  - Bereitstellung der benötigten Server-Dienste
  - Start der Clients

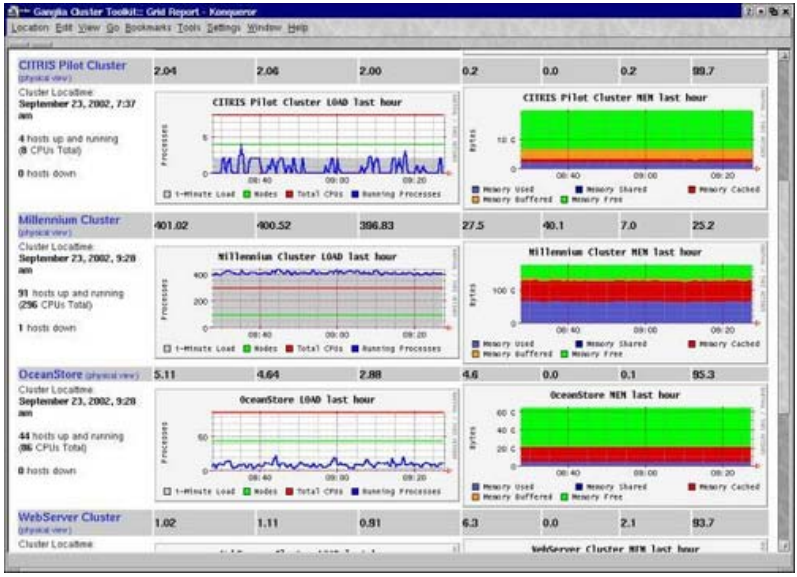
    - Konfiguration des Clusters
- Globus Toolkit 4.0
    - Jobs absetzen per Kommandozeile
    - Jobs absetzen per Web-Service
    - File-Transfer (Reliable FT, GridFTP)
    - Parallelverarbeitung mittels Globus-MPI

3. Planung

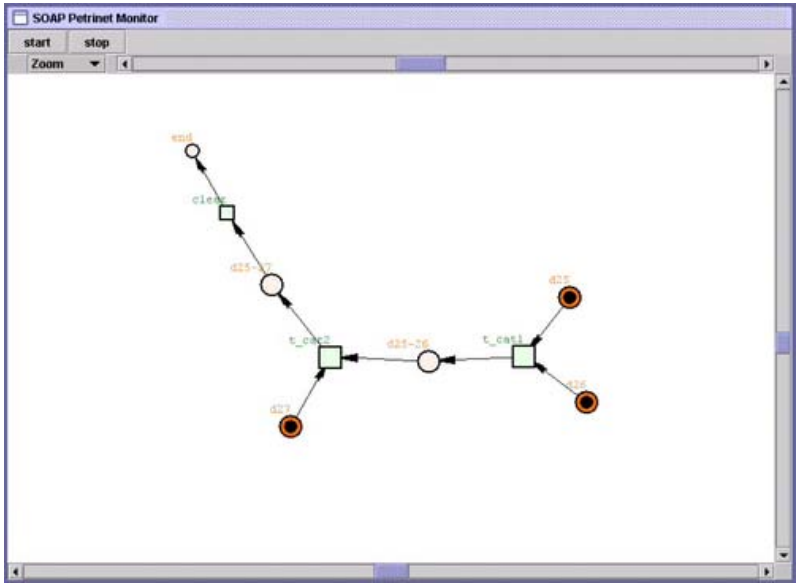
3.1 Geplante Grid-Software

- Gridsphere Portal Framework
- Ganglia Monitoring System
- Grid-Workflow-Management

Die Grundlage des Instant-Grid-Portals ist Gridsphere, ein vom Albert-Einstein-Institut in Potsdam entwickelter Java-Portlet-Server. Zur Überwachung der Instant-Grid-Clients wird Ganglia eingesetzt:



Die Verwaltung der Grid-Jobs soll mittels eines vom Fraunhofer-Institut für Rechnerarchitektur und Softwaretechnik entwickelten und an das Instant-Grid angepassten Job-Managers erfolgen:

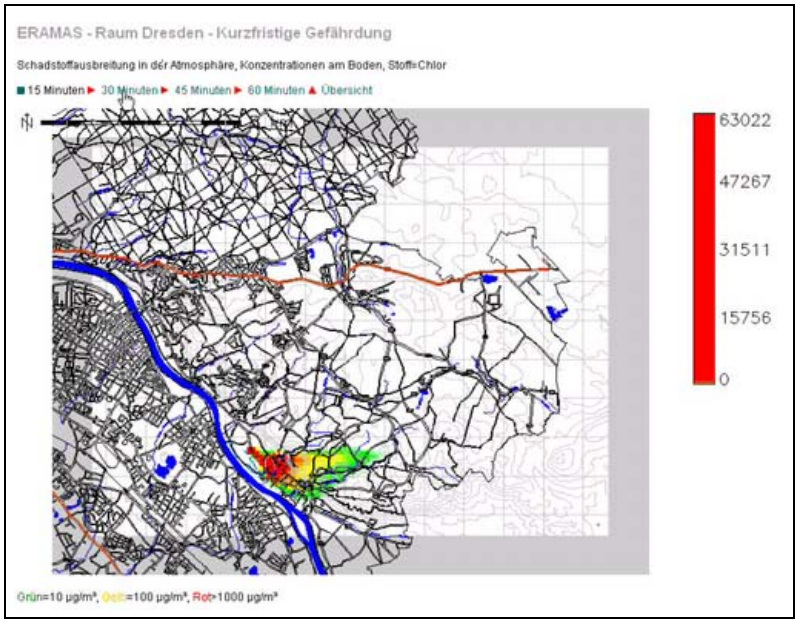


3.2 Geplante Demo-Anwendungen

Die geplanten Demo-Anwendungen sind ein besonders wichtiges Element des Instant-Grid-Projektes, da nur mit ihrer Hilfe die Grid-Funktionalität Einsteigern in die Materie zugänglich gemacht werden kann. Geplant sind zur Zeit folgende Anwendungen:

- Eramas (Schadstoffausbreitung), bereitgestellt vom Fraunhofer-Institut für Rechnerarchitektur und Softwaretechnik
- Gridlab (Reale Experimente in virtuellen Räumen), bereitgestellt von der Fernuniversität Hagen
- AccessGrid (Kollaborationswerkzeuge)
- Povray (verteiltes Raytracing)

Zum Beispiel kann mit Eramas die Ausbreitung von Schadstoffen nach einem fiktiven Chemie-Unfall berechnet werden. Die Parameter des Unfalls können vom Nutzer innerhalb des Portals variiert werden:



Anschließend erfolgt die Berechnung im Instant-Grid, wobei die Verteilung der Aufgaben auf die Clients mit Ganglia und dem Job-Manager sichtbar gemacht wird.

4. Die Instant-Grid-Webpräsenz

Weitere Informationen zum Instant-Grid-Projekt befinden sich auf der Webpräsenz www.instant-grid.de. Dort können auch aktuelle ISO-Images herun-

tergeladen werden. Außerdem stehen Foren und ein Kontaktformular zur Verfügung. Eine Online-Dokumentation ist im Aufbau.

NPS in den Instituten – Bericht vom Workshop

Petra Küster

Max-Planck-Institut für biophysikalische Chemie, Göttingen

1. Nutzung von NPS in der MPG

Die GWDG betreut und administriert in Göttingen das Redaktionssystem **cms.mpg.de** mit dem Content-Management-System NPS 5. Dort werden die Webseiten der Max-Planck-Gesellschaft **www.mpg.de** gepflegt. Die Inhalte werden zum einen durch die Pressestelle der MPG eingestellt, zum anderen durch die Institute über den Stammdateneditor.

Mittlerweile gibt es 11 Max-Planck-Institute, die für ihren Webauftritt dieses Redaktionssystem nutzen.

8 Institute sind online:

- MPI für Biogeochemie (www.bgc-jena.mpg.de)
- MPI für Biophysikalische Chemie (www.mpibpc.mpg.de)
- MPI für Dynamik und Selbstorganisation (www.ds.mpg.de)
- MPI für Eisenforschung (www.mpie.de)
- MPI für Gravitationsphysik (www.aei.mpg.de)

- MPI für Kolloid- und Grenzflächenforschung (www.mpikg.mpg.de)
- MPI für Neurobiologie (www.neuro.mpg.de)
- MPI für Züchtungsforschung (www.mpiz-koeln.mpg.de)

3 Institute arbeiten noch an ihrem Webauftritt:

- MPI für Biochemie
- Kunsthistorisches Institut
- Radioastronomie

Außerdem gibt es 2 Spezialwebseiten von Instituten:

- Komm-ins-Beet (komm-ins-beet.mpg.de)
- Einstein Online (www.einstein-online.info)

Neben dem Redaktionssystem bei der GWDG gibt es 2 Institute, die eigene NPS-Server betreiben:

- Institut für Plasmaphysik
- MPI für medizinische Forschung

Unter der MPG-Sitelizenz entstehen für einen eigenen NPS-Server keine Lizenzkosten.

2. Warum haben sich Institute für NPS entschieden?

Das für die Webseiten empfohlene Corporate Design ist sehr komplex. Im NPS stehen viele Templates zur Verfügung, die dieses umsetzen. Es ist ein „Baukasten“ von Templates und Objekten vorhanden, der ein Grundgerüst von Webseiten erzeugt.

Die meisten Institute haben sich entschieden, das vorhandene CMS-System zu nutzen, das von der GWDG gepflegt wird. Zum einen sind so Zugriffe auf Inhalte möglich, die mit dem Stammdateneditor eingepflegt werden. Einige Webseiten mit Informationen zur Geschichte, Organisation und Profil des Instituts sind damit gleich fertig gestellt. Zum anderen spart man sich durch die Nutzung des Redaktionssystems administrativen Aufwand, außerdem ist die Nutzung, abgesehen von Arbeitseinheiten, kostenlos.

Nach dem Export der Webseiten ist eine Synchronisation mit dem institutseigenen Webserver möglich. Viele Institute haben sich entschieden, auch den Webserver von der GWDG hosten zu lassen.

3. Schwierigkeiten beim Arbeiten mit NPS

Auch wenn viele Templates und Objekte vorhanden sind, ist eine Anpassung nötig, bevor man mit der Redaktionstätigkeit, d. h. das Einpflegen von Inhalten, beginnen kann. Dazu kommt die Tatsache, dass die Templates aufgrund des komplexen Corporate Designs sehr kompliziert sind und einige Templates, z. B. für Seminare, fehlen.

Das Ganze muss man vor dem Hintergrund sehen, dass die Verantwortlichkeit für die Webseiten bei vielen Instituten im Bereich der Öffentlichkeitsarbeit liegt. Diese Mitarbeiter haben in der Regel nicht die Zeit oder das Know-how, sich in die Logik der Templates einzuarbeiten. Aus diesem Grund haben viele Institute die Realisierung ihrer Webseiten außer Haus gegeben, damit sich die Mitarbeiter der Öffentlichkeitsarbeit auf das Einstellen der Inhalte konzentrieren können. Nur Institute, in denen auch Mitarbeiter mit EDV-Erfahrung involviert waren, haben die Umsetzung ihres Webauftritts mit NPS eigenständig realisiert.

Diese „Power User“ stören die eingeschränkten Rechte auf dem Redaktionssystem. Jeder kann zwar seine Templates bearbeiten, aber Änderungen in den Objekten, z. B. zusätzliche Attribute oder Systemjobs, können nur von dem Administrator des Systems gemacht werden.

4. Das Redaktionssystem

Die Hardware ist zur Zeit überlastet, so dauert der tägliche Export der Seiten (ca. 25 GB) und das Backup über 10 Stunden. Es gibt nur einen Server, sodass Testmöglichkeiten begrenzt sind, da immer das Produktionssystem betroffen ist. Außerdem ist noch die ältere Version NPS 5 im Einsatz.

Zur Zeit werden 2 neue Server beschafft, ein Server für das Produktionssystem (mit 4 Dual-Core Prozessoren) und ein zweiter Server für das Testsystem (mit 4 Single-Core-Prozessoren). Auf den neuen Servern wird NPS 6 installiert.

5. Vorteile von NPS 6

- Die Bedienung durch Redakteure ist durch „Inline Editing“ intuitiv, dabei wird direkt in der Webansicht editiert. Damit verringert sich der Schulungsaufwand der Redakteure.
- Eine Ansicht der Objekte in einer Baumstruktur, ähnlich dem Explorer, erlaubt eine leichtere Bearbeitung mehrerer Objekte.
- Es gibt eine einfache Möglichkeit, alle externen Links zu überprüfen.

- In NPS 6 können für Institute Instanzen aufgesetzt werden, sodass jedes Institut in seinem Bereich Administratorrechte hat.
- Der Export kann auf die veränderten Seiten eingeschränkt werden und wird damit sehr beschleunigt.
- Es wird Versionierung geben. Dies war zwar schon unter NPS 5 möglich, war auf dem Redaktionssystem aber nicht eingeschaltet.

6. Initiative der NPS-Nutzer

Im Rahmen eines Workshops während des DV-Treffens gab es einen ersten Erfahrungsaustausch. Die Zeit war aber viel zu kurz, um alle anliegenden Themen ausreichend diskutieren zu können. Daher ist für Februar ein Anwender-Treffen geplant. Ziel ist es, Lösungen, z. B. Templates, auszutauschen, damit die gleiche Arbeit nicht mehrfach gemacht wird. Dringend benötigt wird auch eine Anleitung für „Anfänger“, damit kleinere Institute NPS benutzen können, ohne externe Berater finanzieren zu müssen.

Die Helmholtz-Gemeinschaft deutscher Forschungszentren und ihre IT-Landschaft

Klaus-Peter Mickel [1]

Forschungszentrum Karlsruhe, Institut für Wissenschaftliches Rechnen [2]

1. Einleitung

„Ein deutscher Forschungsriese begibt sich auf Expansionskurs“ – mit dieser Schlagzeile hat die Frankfurter Allgemeine Zeitung am 16.11.2005 die Helmholtz-Gemeinschaft deutscher Forschungszentren (HGF) einigermaßen treffend beschrieben. Die HGF ist mit 24.000 Beschäftigten und einem Jahresbudget von 2,25 Milliarden Euro außerhalb der Universitäten die mit Abstand größte Forschungsorganisation Deutschlands. In dem folgenden Beitrag werden die Kernaufgaben der 15 in der HGF zusammengeschlossenen deutschen Forschungszentren beleuchtet sowie zwei herausragende Beispiele der IT-Infrastruktur der HGF vorgestellt.

1. mickel@iwr.fzk.de
2. http://www.fzk.de/iwr

2. Die HGF – Zahlen, Fakten, Themen

Unter dem Dach der Helmholtz-Gemeinschaft [3] haben sich 15 deutsche Forschungszentren zusammengeschlossen, für die gelegentlich auch das Attribut „Großforschung“ verwendet wird. In der Tat sind einige dieser Zentren sehr groß: Im Deutschen Zentrum für Luft- und Raumfahrt (DLR) sowie in den Forschungszentren Jülich (FZJ) und Karlsruhe (FZK) sind jeweils etwa 4.000 Personen beschäftigt, so dass diese drei Zentren zusammen bereits die Hälfte der gesamten HGF ausmachen. Bei allen Helmholtz-Zentren finanziert der Bund jeweils 90 Prozent der öffentlichen Zuwendungen, das Bundesland, in dem ein HGF-Zentrum seinen Sitz hat, steuert jeweils die restlichen 10 Prozent bei. Bei nahezu allen Zentren kommen in erheblichem Umfang Drittmittel hinzu.

Die in der HGF bearbeiteten Forschungsschwerpunkte grenzen sich deutlich ab von den Themen der anderen großen deutschen Forschungsorganisationen: Während in der Max-Planck-Gesellschaft vorwiegend Grundlagenforschung betrieben wird und die Fraunhofer-Gesellschaft sich überwiegend anwendungsnahen Entwicklungen widmet, liegen die Schwerpunkte der HGF – mit einigen Ausnahmen – zwischen diesen beiden Extremen. In der HGF werden gemäß der „HGF-Mission“ [4] große und drängende Fragen von Gesellschaft, Wissenschaft und Wirtschaft sowie Systeme hoher Komplexität erforscht, wobei der Einsatz wissenschaftlicher Großgeräte und großer leistungsfähiger wissenschaftlicher Infrastrukturen als Alleinstellungsmerkmal eine wesentliche Rolle spielt. Die von den etwa 8.500 Wissenschaftler(inne)n der HGF in 250 Instituten bearbeiteten Forschungsvorhaben sind in die Forschungsbereiche Energie, Erde und Umwelt, Gesundheit, Schlüsseltechnologien, Struktur der Materie sowie Verkehr und Weltraum gegliedert.

3. Großgeräte in der HGF

Der Betrieb, die Nutzung und das Zur-Verfügung-Stellen wissenschaftlicher Großgeräte ist eine wesentliche Aufgabe der Helmholtz-Gemeinschaft, da im allgemeinen weder Universitäten noch Institute anderer Forschungsorganisationen für solche großen Vorhaben gerüstet sind. Einige dieser von HGF-Instituten betriebenen oder geplanten Großgeräte werden im folgenden vorgestellt: Das Forschungsschiff Polarstern, das Forschungsflugzeug HALO,

3. http://www.helmholtz.de

4. http://www.helmholtz.de/de/Wir_ueber_uns/Mission.html

das Neutrino-Experiment KATRIN sowie der Freie Elektronenlaser XFEL. Auch besonders leistungsfähige Rechenzentren zählen zu diesen wissenschaftlichen Großgeräten; als Beispiele werden hier das John von Neumann Institute for Computing (NIC) sowie das Grid Computing Centre Karlsruhe (GridKa) genannt.

3.1 Das Forschungsschiff Polarstern [5]

Das Alfred-Wegener-Institut in Bremerhaven (AWI) betreibt das Polarforschungsschiff Polarstern, das als wichtigstes Werkzeug der deutschen Polarforschung und als leistungsfähigstes Polarforschungsschiff der Welt gilt. Dieses 118 m lange Schiff ist als doppelwandiger Eisbrecher konstruiert und kann deshalb 1,5 Meter dickes Eis mit einer Geschwindigkeit von ca. 5 Knoten durchfahren. Es kann bei Außentemperaturen bis zu -50 ° C arbeiten und sogar in polaren Regionen überwintern. Die Polarstern bietet Arbeitsmöglichkeiten für bis zu 50 Wissenschaftler und Techniker.

Das Schiff ist für biologische, geologische, geophysikalische, glaziologische, chemische, ozeanographische und meteorologische Forschungsarbeiten ausgerüstet und verfügt über neun wissenschaftliche Labors. Zusätzliche Laborcontainer können auf und unter Deck gestaut werden. Kühlräume und Aquarien erlauben den Transport von Proben und lebenden Meerestieren.

Forschungsgeräte und Messinstrumente werden mit Hilfe von Kränen und Winden ausgebracht und bis in große Tiefen herabgelassen. Spezielle Vermessungslote, die bis in 10.000 Meter Tiefe reichen und bis 150 Meter in den Meeresboden eindringen können, stehen für wissenschaftliche Untersuchungen zur Verfügung. Das Bordrechnersystem erfasst und speichert laufend meteorologische, ozeanographische und weitere Daten nach Bedarf.

3.2 Das Forschungsflugzeug HALO [6]

Das Deutsche Zentrum für Luft- und Raumfahrt (DLR) koordiniert seit 2004 die Planungen und Entwicklungen für den Bau des Forschungsflugzeuges HALO (High Altitude and Long Range Research Aircraft). HALO, ein hochmodernes wissenschaftliches Großgerät, das 2008 zu seinem Erstflug starten soll, wird bei nahezu allen wichtigen Parametern die Leistungsfähigkeit aller bisher weltweit operierenden Forschungsflugzeuge übertreffen: Bei einer Flughöhe von mehr als 15 Kilometern, einer Nutzlast von drei Tonnen

5. http://www.awi-bremerhaven.de/Polar/polarstern-d.html
6. http://www.halo.dlr.de/

und einer Reichweite von über 8000 Kilometern sind damit erstmals Messungen auf der Skala von Kontinenten, auf allen Breiten, von den Tropen bis zu den Polen sowie in Höhen bis zur unteren Stratosphäre möglich. HALO wird eine bisher unerreichte Qualität von Messungen gerade in den für das Leben auf der Erde so bedeutsamen Höhenschichten der Atmosphäre bieten. Damit wird auch ein wesentlicher Beitrag zum Verständnis der Ozonproblematik und des Austauschs von Luftschadstoffen geleistet. HALO soll vor allem in der Troposphäre und der unteren Stratosphäre Messungen durchführen und für Erdbeobachtungen eingesetzt werden. Zu den Forschungsschwerpunkten von HALO werden u. a. Untersuchungen zu den Ursachen von Extremwetterereignissen sowie zu den Selbstreinigungsprozessen in der Atmosphäre zählen.

3.3 Das Neutrino-Experiment KATRIN [7]

KATRIN, das KArlsruhe TRItium Neutrino Experiment, entsteht gegenwärtig als Großexperiment der Elementarteilchenphysik am Forschungszentrum Karlsruhe (FZK). Sein Ziel ist die Bestimmung der Neutrino-Ruhemasse mit einer Genauigkeit von nur 0,2 eV. Die erst vor wenigen Jahren nachgewiesene Existenz der Neutrinomasse ist von sehr erheblicher Bedeutung für die Teilchenphysik, die Astrophysik und ganz besonders für die Kosmologie. Die kosmologische Forschung geht davon aus, dass das Weltall milliardenfach mehr Neutrinos als Protonen und Neutronen enthält, so dass eine auch nur geringe Neutrinomasse einen erheblichen Anteil an der Masse des Weltalls hätte. Die Kosmologie kann heute nur etwa 5 Prozent der Masse des Weltalls erklären, die restlichen 95 Prozent sind unbekannt und werden deshalb noch immer als „Dunkle Materie“ und „Dunkle Energie“ bezeichnet. Hier erhofft man sich von KATRIN wesentliche Erkenntnisse, die zum Verständnis kosmologischer Vorgänge bis hin zu den Ereignissen in der ersten Nanosekunde nach dem Urknall beitragen sollen.

3.4 Der Freie Elektronenlaser XFEL [8]

Am Deutschen Elektronen-Synchrotron in Hamburg (DESY) wird seit 2004 der Bau und Betrieb eines europäischen „XFEL“ vorbereitet, eines X-Ray Free Electron Lasers, der 2012 betriebsbereit soll. Der wissenschaftlich-technische Clou des XFEL besteht in den damit erzielbaren extrem kurzen, gleichwohl aber extrem energiereichen Röntgenlichtblitzen. Realisiert wird

7. http://www-ik.fzk.de/~katrin/index.html
8. http://xfel.desy.de/

der XFEL in Form eines 3,4 km langen unterirdischen Linearbeschleunigers mit mehreren Messstationen.

Mit dem XFEL wird es gelingen, in bislang unerreichte atomare Dimensionen vorzustoßen: Seine Leuchtstärke ist in ihren Spitzenwerten milliardenfach höher als bei heutigen Röntgenquellen; die mittlere Leuchtstärke ist zehntausendfach höher. Seine Zeitauflösung ist um Größenordnungen besser als die bisher verfügbarer Quellen – ein Röntgenblitz ist kürzer als 100 Femtosekunden; das ist die Zeitdauer, in der sich chemische Bindungen ausbilden und Molekülgruppen ihre Lage ändern. Die Wellenlänge seines Röntgenlichts ist so klein, dass selbst atomare Details erkennbar werden. Sie kann im Bereich zwischen sechs und einem Zehntel Nanometer variiert werden. Seine Röntgenstrahlung hat die Eigenschaften von Laserlicht. Damit sind beispielsweise holographische Aufnahmen auf atomarer Ebene möglich.

Die unvorstellbar kurzen und intensiven Röntgenpulse ermöglichen es den Forscherinnen und Forschern, chemische Reaktionen mit atomarer Auflösung regelrecht zu filmen, ebenso auch die Bewegungen von Biomolekülen oder die Entstehung von Feststoffen aufzunehmen. Davon profitieren die verschiedensten Naturwissenschaften – von der Physik über die Chemie, die Material- und Geoforschung bis hin zu den Biowissenschaften. Ebenso nutzen industrielle Anwender diese neuen Erkenntnisse, beispielsweise wenn es darum geht, neue Werkstoffe und Materialien im Nanobereich zu entwickeln – also mit Abmessungen von Milliardstel Metern.

3.5 Das John von Neumann Institute for Computing (NIC) [9]

Das John von Neumann-Institut für Computing (NIC) ist eine gemeinschaftliche Gründung des Forschungszentrums Jülich (FZJ) und des Deutschen Elektronen-Synchrotron (DESY) und dient der Förderung der supercomputergestützten naturwissenschaftlich-technischen Forschung und Entwicklung. Eine sehr wesentliche Aufgabe des NIC besteht in der Bereitstellung von Supercomputerkapazität für bundesweit laufende Projekte der Wissenschaft, Forschung und Industrie auf dem Gebiet der Modellierung und Computersimulation. Daneben wird am NIC Supercomputerorientierte Forschung und Entwicklung auf ausgewählten Gebieten der Physik und anderer Naturwissenschaften betrieben. Für die Wissenschaftler stehen im John von Neumann-Institut für Computing umfangreiche Rechnerressourcen bereit. Der z. Zt. (Nov. 2005) leistungsstärkste Computer des NIC ist das

9. http://www.fz-juelich.de/nic/

IBM p690-Cluster JUMP; im ersten Quartal 2006 wird ein fünfmal stärkeres Cluster des Typs IBM Blue Gene/L hinzukommen.

JUMP (JUelich Multi Prozessor) wurde Anfang 2004 installiert. Mit seinen 1.312 Prozessoren (41 Knoten mit je 32 Prozessoren) erreicht er eine Peak Performance von 8,9 TeraFlop/s. Er verfügt über 5 Terabyte Hauptspeicher und 56 Terabyte Plattenspeicher. Das Cluster des Typs IBM Blue Gene/L, das am NIC in Jülich Anfang 2006 in Betrieb gehen soll, wird insgesamt 8.192 Knoten mit je zwei Prozessoren umfassen. Dieser Rechner wird eine Peak Performance von 45,8 TeraFlop/s erreichen und damit voraussichtlich für einige Zeit zum leistungsstärksten zivil genutzten Supercomputer der Welt werden.

3.6 Das Grid Computing Centre Karlsruhe (GridKa) [10]

Im Forschungszentrum Karlsruhe (FZK) entsteht seit 2002 das Grid Computing Centre Karlsruhe (GridKa). Zusammen mit zehn anderen sehr großen und mehr als 100 mittelgroßen Rechenzentren auf allen Kontinenten ist GridKa ein wesentlicher Teil des weltumspannenden Computing- und Daten-Grid, mit dessen Hilfe die internationale Community der Elementarteilchenphysiker die Experimente großer Teilchenbeschleuniger auswerten will. Besonders im Focus steht dabei der Large Hadron Collider LHC [11], ein gigantisch großer Protonenbeschleuniger, der am Europäischen Kernforschungszentrum CERN bei Genf 2008 in Betrieb gehen wird. Der LHC wird jährlich 10 Petabyte Messdaten liefern, die in diesem globalen Grid ausgewertet werden sollen. GridKa umfasst schon heute ca. 2.000 Prozessoren (überwiegend AMD-Opteron), ein Terabyte Hauptspeicher, etwa 500 Terabyte Online-Disk sowie ein Bandarchiv mit einer Kapazität von einem Petabyte. Die Verbindung zum Internet und eine Standleitung zum CERN haben jeweils eine Bandbreite von 10 Gigabit/Sek.

GridKa betreibt schon heute das umfangreichste Rechen- und Daten-Cluster in der deutschen Wissenschaftslandschaft, obwohl erst etwa zwanzig Prozent des für 2008 vorgesehenen Endausbaus erreicht sind. Dann werden bei GridKa mehr als 5.000 Prozessoren in Betrieb sein, mehr als 4,5 Petabyte Online-Datenspeicher sowie an die 10 Petabyte Bandarchiv – aus heutiger Sicht sind das nahezu unvorstellbare Größenordnungen. Die Computer und Speichermedien werden mehr als ein Megawatt an elektrischer Leistung auf-

10. http://www.gridka.de

11. http://www.cern.ch/lhc

nehmen, die (leider) in Form von Wärme wieder abgeführt werden müssen. Die Bandbreiten der Datenleitungen zum CERN und zu den anderen in aller Welt beteiligten Rechenzentren werden insgesamt 30 Gigabit/Sek erreichen. Mannigfache softwaretechnische Herausforderungen kommen noch hinzu: Weltweit verteilte Datenbanken im Petabyte-Maßstab, Batchsysteme, die Jobs sinnvoll auf mehr als 100.000 Prozessoren in aller Welt verteilen müssen, hochkomplexe Sicherheitsmechanismen, die Verwaltung von 8.000 weltweit verteilten Nutzern, die jedoch im Prinzip alle auf allen 100.000 Prozessoren rechnen können – das alles sind Herausforderungen, die es in diesem Umfang weltweit bisher noch nie gegeben hat.

4. Beteiligung von HGF-IT-Abteilungen an nationalen Projekten: DFN [12] und D-Grid [13]

Selbst eine oberflächliche Beschreibung der IT-Landschaft der Helmholtz-Zentren wäre ohne Erwähnung einiger nationaler IT-Projekte unvollständig, an denen sich jeweils mehrere oder gar alle IT-Abteilungen der HGF beteiligen. Das Deutsche Forschungsnetz DFN ist dafür ein gutes Beispiel. Vor mehr als zwanzig Jahren als Selbsthilfeeinrichtung der deutschen Wissenschaft gegründet, ist das DFN heute der unumstrittene nationale Datennetzbetreiber für alle deutschen wissenschaftlichen Einrichtungen; unabhängige Gutachter bezeichnen es seit vielen Jahren als das technisch beste Forschungsnetz weltweit. Mehrere HGF-Zentren gehörten 1985 zu den Gründungsmitgliedern des DFN, bis heute sind ausnahmslos alle Helmholtz-Einrichtungen DFN-Mitglieder und -Nutzer. Die Bandbreite der jeweiligen Anschlüsse richtet sich nach dem Bedarf der Zentren und reicht von 155 Mbit/Sek bis zu 10 Gbit/Sek. Immerhin drei Helmholtz-Zentren sind mit einer Bandbreite von 1 Gbit/Sek mit dem Internet verbunden.

Seit Herbst 2005 beteiligen sich zahlreiche IT-Abteilungen von HGF-Zentren an der deutschen Grid-Initiative D-Grid. Unter diesem Kürzel fördert das Forschungsministerium BMBF [14] eine Vielzahl von Grid-Projekten, um so die namhaften IT-Betreiber und -Anwender aus den deutschen wissenschaftlichen Communities auf dem innovativen Gebiet des Grid Computing im globalen Wettbewerb zu unterstützen. Erwähnenswert ist u. a. das D-Grid-Integrationsprojekt, dessen Aufgabe darin besteht, bis 2008 eine bun-

12. http://www.dfn.de

13. http://www.d-grid.de

14. http://www.bmbf.de

desweit verfügbare, robuste, zuverlässige und nachhaltig nutzbare Grid-Infrastruktur bereitzustellen und zu betreiben. Dieses "Kern-D-Grid" wird dann allen interessierten wissenschaftlichen Communities in Deutschland für die Nutzung zur Verfügung stehen. Außerdem werden derzeit sechs "Community-Grids" gefördert, welche fachspezifische Anwendungen für die Nutzung in einer (weit-)verteilten Grid-Umgebung ertüchtigen. An den D-Grid-Projekten und insbesondere am Integrationsprojekt sind Helmholtz-Zentren maßgeblich beteiligt, mehrere D-Grid-Konsortien werden von Helmholtz-Zentren koordiniert.

5. Zusammenfassung

Die in der Helmholtz-Gemeinschaft deutscher Forschungszentren zusammengefassten 15 deutschen Forschungseinrichtungen bilden mit einem Jahresbudget von 2,25 Milliarden Euro die größte Forschungsorganisation Deutschlands. Großforschung mit gesellschaftlicher Relevanz ist eines ihrer wichtigen Themen, Betrieb und Nutzung wissenschaftlicher Großgeräte von internationaler Bedeutung kommen ebenso hinzu wie leistungsfähige wissenschaftliche Infrastrukturen und starke Partner aus Wissenschaft und Industrie. In diesem Beitrag wurde die nachhaltige Bedeutung der Helmholtz-Gemeinschaft für die deutsche und die internationale Wissenschaft verschiedener Disziplinen an Hand der Großgeräte Polarstern, HALO, KATRIN und XFEL sowie der Groß-Rechenzentren NIC und GridKa dargestellt.

Telefonieren nur noch über das Internet? – Erfahrungsbericht zum aktuellen Hype „Voice over IP“ (VoIP)

Heinz Junkes

Fritz-Haber-Institut der Max-Planck-Gesellschaft, Berlin

Zur Zeit findet man in vielen Medien Berichte, dass VoIP aus seinen Kinderschuhen herausgewachsen sei und nicht nur im privaten Bereich (Systeme wie z. B. Skype), sondern auch in der Geschäftswelt eingesetzt werden sollte. Auch in der Max-Planck-Gesellschaft wird der Eindruck erweckt, dass VoIP die Zukunft sei und neue Sprachsysteme nur noch auf Basis von Übertragungstechnologien der Datennetze aufgebaut werden sollten. Als Grund wird vor allem die Kostenersparnis durch die gemeinsame Nutzung der Dateninfrastruktur hervor gebracht. Ich werde in diesem kurzen Erfahrungsbericht meine Sicht der Dinge zu VoIP darlegen und die Konsequenzen, die sich dadurch für das Fritz-Haber-Institut (FHI) ergaben, erläutern.

Am FHI betreiben wir seit über zehn Jahren ein Telefonsystem der Firma Alcatel (4400, heute OmniPCX), welches als Betriebssystem Unix (Chorus, jetzt Mandrake-Linux) einsetzt (siehe Abb. 1).

Abb. 1: Telefonanlage

Das System ersetzte eine in die Jahre gekommene Anlage auf Relais-Basis. Das neue TK-System war eine der ersten Anlagen, die auf einem normalen Unix-Betriebssystem basierte. Darum wurde die Installation und der Betrieb von der IT-Gruppe am FHI übernommen. Dies war zum damaligen Zeitpunkt noch sehr ungewöhnlich, da TK-Anlagen wohl aus historischen Gründen eher von der Haustechnik (da „BAU“-zugehörig) betreut wurden.

Bei der Erstinstallation wurden die bestehenden eigenen Kupferkabelverbindungen der alten Installation übernommen. Sämtliche Telefonapparate wur-

den ausgetauscht, da die neuen mit einem digitalen Übertragungsprotokoll (UA-Schnittstelle) mit dem zentralen Telefonsystem kommunizieren. Die Anzahl der analogen Anschlüsse wurde stark reduziert (< 20 am ganzen Institut).

Das TK-System baut auf einer universellen Transportinfrastruktur (Alcatel Cyrstal Technology, ACT) auf. Dabei handelt es sich um ein blockierungsfreies, digitales Koppelnetz, das auf Basis dezentraler Intelligenz innerhalb eines peripheren Leiterplattenträgers realisiert wurde. Die Systemarchitektur wird dabei durch die Vernetzung aller Systemkomponenten in Form einer vollständigen Masche gebildet, d. h. von jeder internen Baugruppe ist eine physikalische Leitung zu jeder anderen Baugruppe vorhanden. Eine ACT-Struktur ist auf 28 Leiterplatteneinschübe begrenzt, größere Konfigurationen werden durch Kopplung mehrerer Grundmodule gebildet, es entsteht ein so genanntes Cluster.

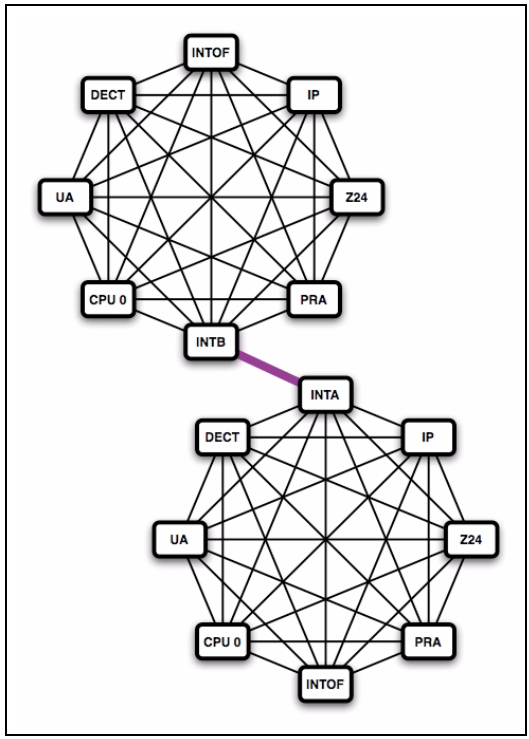


Abb. 2: ACT-Struktur

Die Telefone verfügten von Anfang an über Displays und moderne Leistungsmerkmale wie z. B. Zugriff per Tastatur auf ein zentrales Telefonver-

zeichnis (siehe Abb. 3). Es bestand eine komplette DECT-Funkversorgung des FHI-Campus (incl. Harnackhaus und Archiv der MPG).

Abb. 3: Systemtelefon

Die Anlage wurde stetig modernisiert und erweitert. Durch die ACT-Struktur konnten wir die Anlage kostenoptimiert modular ausbauen und die inzwischen aufgebaute Strukturierte Verkabelung auch zum Anschluss von Telefonen nutzen. Dabei kamen Voice-Hub's (Remote-ACT) zum Einsatz, die als Etagenverteiler installiert wurden (siehe Abb. 4).

Abb. 4: Voice-Hub

Damit wurde eine Infrastruktur geschaffen, die komplett auf klassische Kupferverkabelung verzichtet und mit der Datennetzverkabelung identisch ist. Es ist weiterhin eine zentrale Administration möglich und moderne Dienste wie Anbindung des Telefonverzeichnis an LDAP, Load-Balance und Hot-Swap sind bei TK-Anlagen Standardfunktionen.

Die Anbindung an das öffentliche Netz erfolgt am FHI durch 2 Primärmultiplexanschlüsse (PMX, je 30 Sprachkanäle). Bemerkenswert bei TK-Anlagen ist die sehr hohe Verfügbarkeit. In unserem Fall beläuft sich die Ausfallzeit auf ca. 1 Stunde in 10 Jahren bei der Gesamtanlage. Dies wird gewährleistet durch Funktionen, wie z. B. Upgrade des Betriebssystems zuerst auf die Standby-CPU, dann Synchronisation der Haupt-CPU u. ä.

Um nun VoIP-Funktionen auszutesten und weiterhin den Anschluss an das öffentliche Fernsprechnetz (mit mehr als 2 Mrd. Teilnehmern (Festnetz und Mobil)) zu nutzen, haben wir uns entschlossen, die bestehende Anlage „IP-fähig“ zu machen und keine Komplettumstellung zu wagen, da die damit verbundenen Kosten und die technischen Hindernisse bei der Implementierung uns zu hoch erschienen.

Eine VoIP-Architektur ist sehr komplex. Es müssen viele unterschiedliche Protokolle zusammenspielen. Angefangen bei der Spachkodierung- und komprimierung mit G.711 (PCM) und G.723 (MP-MLQ) über Real Time Transport Protocol (RTP) und Real Time Control Protocol (RTCP) bis zum User Datagram Protocol (UDP), Internet Protocol (IP), Ethernet etc.. Insbesondere das Problem der bei IP fehlenden Signalisierung ist noch zu lösen. Zur Signalisierung werden Protokolle benötigt, die auch zur Vermittlung und Aushandlung von grundlegenden Parametern für die Sprachkommunikation zwischen den beteiligten Partnern dienen. Die wichtigsten Standards für diese Protokolle sind H.323 (ursprünglich für Videokonferenzen im LAN entwickelt) und das Session Initiation Protocol / Session Description Protocol (SIP/SDP). Zusätzliche Protokolle sind z. B. RSVP (Resource Reservation Protocol) für Dienstgüte-Anforderungen, TRIP (Telephony Routing over IP) zum Ermöglichen von Telefongesprächen zwischen verschiedenen Providern oder Diameter zur Autorisierung, Authentifizierung und zum Accounting. Es bleibt aber immer noch das Problem der Umsetzung von IP-Adressen in Telefonrufnummern und umgekehrt. Diese Umsetzung erfolgt bisher meist proprietär.

Wir haben die bestehende Anlage um ein Codec-Board (basierend auf digitalen Signalprozessoren (DSP)) erweitert und mehrere IP-Telefone (siehe Abb. 5) angeschafft.

Abb. 5: IP-Telefon

Um auch bei der IP-Telefonie eine gute Sprachqualität erreichen zu können, wurde vom Hersteller empfohlen, die TK-Anlage sowie die IP-Telefone in ein eigenes Netz-Segment zu legen. Nur damit kann der dafür vorgesehene Quality of Service (QoS) erreicht werden.

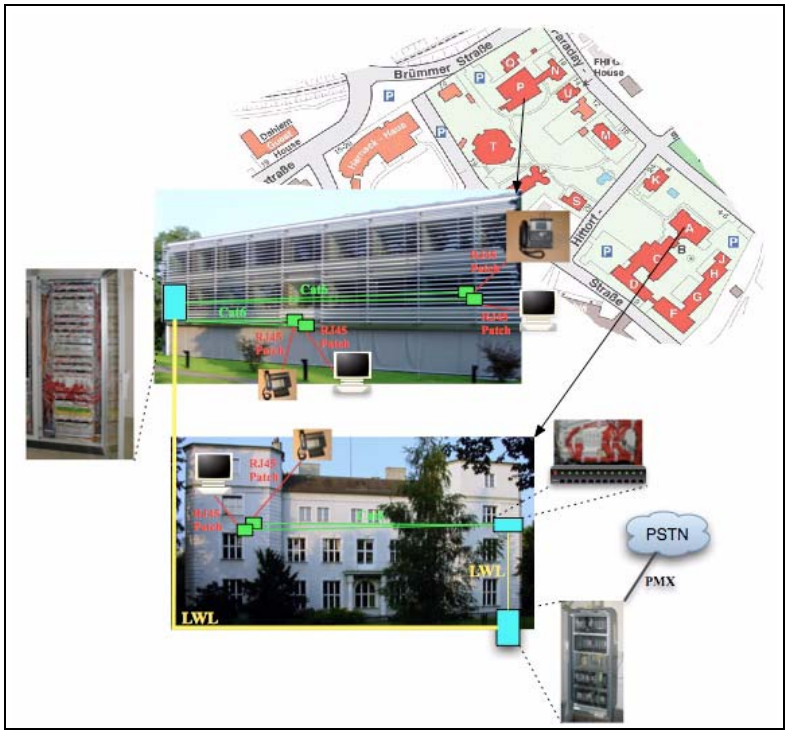


Abb. 6: „Telefonie nutzt Strukturierte Verkabelung“

Dies hätte aber in unserem Fall bedeutet, dass wir den Großteil unserer aktiven Datennetz-Geräte (Switches) austauschen müssten. Bei Sprachverbindungen ist es wichtig, die Signale isochron zu übertragen, um keine Verzerrungen (Jitter, Varianz der Paketlaufzeiten) zu erhalten, die die Übertragung stark stören. Beim Jitter treffen Pakete, die in gleichmäßigen Intervallen in das Netz gesendet werden, in unregelmäßigen Abständen oder vertauschter Reihenfolge beim Empfänger ein. Ist ein Paket zu schnell am Ziel, kann es sein, dass es nicht ordentlich dekodiert werden kann oder gar verworfen werden muss, weil das vorhergehende Paket noch verarbeitet wird. Kommt es dagegen später als erwartet beim Empfänger an, könnten Lücken in der Sprachwiedergabe entstehen. Dem Jitter kann man durch den Einsatz eines Jitter-Buffers an den Endpunkten entgegenwirken.

Die Paketlaufzeiten sind natürlich bei einer bestehenden Ethernet-Infrastruktur nicht vorhersehbar. Auch der Einsatz von dynamischen Virtuellen Lokalen Netzen (V-LAN), der es ermöglichen würde, die IP-Telefone wahlfrei an

den Netzanschlussdosen betreiben zu können, ist in einem existierenden Netz nicht ohne weiteres möglich. Dies sind Randbedingungen, die bei den VoIP-Systemen der Datennetzanbieter (Cisco, 3Com, Shoreline, Vertical Networks) in besonderem Maße zu erfüllen sind.

Meist kommen auch noch spezielle properitäre Protokolle zum Einsatz, die eine Priorisierung von Sprach-Daten-Paketen ermöglichen sollen. Wir haben uns für den pragmatischen Weg (und den für uns einzig realisierbaren) entschieden und betreiben die Telefone an unserem sehr „Bandbreiten-starken" Datennetz (100 MBit/s Anschluss, 10 GBit/s Backbone) ohne spezielle Konfiguration der aktiven Netzkomponenten.

Die neuen Apparate sind leider bei den Benutzern teilweise auf Ablehnung gestoßen, obwohl die Bedienerführung an die existierenden Apparate angelehnt ist (gleiche Systemfamilie). Dies mag daran liegen, dass die Bedienerführung auf den ersten Blick ungewohnt war. Die neuen Geräte bieten natürlich nun bunte Displays mit einigen Animationen. Die alten Telefone machen einen schlichteren Eindruck. Die Sprachqualität wurde von den Anwendern bemängelt und hier vor allem die mangelhafte *echo cancellation*, die speziell bei Verbindungen mit Mobilfunkteilnehmern sehr oft auftritt, so dass diese Art der Verbindungen stellenweise nicht genutzt werden konnte. Echoeffekte entstehen durch akustische Rückkopplungen zwischen Hör- und Sprechkreis und sind wahrnehmbar, wenn die Verzögerungszeit etwa 25 ms überschreitet. Um diesen Effekt zu unterdrücken, muss in den VoIP-Systemen eine Echokompensation zum Einsatz kommen. Dabei wird das erwartete Echo simuliert und vom realen Echo subtrahiert. Dieses Problem existiert bei der VoIP-Telefonie leider noch allgemein und wird von den großen Tk-Anlagen-Anbietern (Alcatel, Avaya, Mitel, Nortel, Siemens) noch am besten durch die Benutzung von geeigneten Codecs auf den DSP-Karten gelöst. Eine ganz starke Ablehnung mussten wir bei den rechnergestützen Softphones feststellen. Bei diesen IP-Software-Telefonen handelt es sich um normale Arbeitsplatz-PC's, die mit Soundkarte, Lautsprecher und Mikrofon ausgerüstet sind und mit Hilfe einer Client-Software um die Telefon-Funktionalität erweitert werden.

Wir konnten durch die IP-Erweiterung der TK-Anlage erreichen, dass das System als SIP-Gateway (SIP, Session Initiation Protocol) arbeiten kann und wir so z. B. Softphones von Reisenden durch Internet-Verbindungen im Nummernraum unserer Anlage integrieren können. Diese haben dann Zugang zum öffentlichen Fernsprechnetz mit der Absenderkennung +49 30 8413 xxxx und sind somit wirklich mobil. Auch die Anbindung von Systemtelefonen am Heimarbeitsplatz über eine DSL-Leitung ist möglich und wird auch genutzt.

Im Vergleich zu den Daten-Netzanbieter stellen die TK-Anlagen der traditionellen Telekommunikationsanbieter alle gewohnten Leistungsmerkmale wie z. B. Namenswahl, Rückruf, Rufweiterleitung, Konferenzen und Voice-Mail zur Verfügung und erlauben es in gewohnter Weise analoge oder sicherheitsrelevante Systeme zu betreiben. Dies beinhaltt z. B. das gute alte Fax (G3), welches in einer Geschäftsumgebung nicht zu verdrängen ist (Ich versuche dies schon seit 10 Jahren und kann mich mit Schmunzeln noch sehr gut an meine ambitionierten Versuche erinnern, FAX-G3 durch das digitale FAX-G4 zur ersetzen, und dann daran, die ganze MPG mit ein oder zwei zentralen, datennetzbasierten Fax-Servern auszurüsten). In der Gebäudeautomatisierung sind z.B Telefone in Fahrstühlen zwingend vorgeschrieben, die natürlich auch bei einem Stromausfall betriebsbereit sein müssen und darum überwacht und von der TK-Anlage den erforderlichen Betriebsstrom erhalten müssen. Viele Fernwartungszugänge (z. B. Stromnetzbetreiber zum Auslesen der Leistungsaufnahme von Transformatoren, Rechenanlagenhersteller etc.), Kreditkartenlesegeräte und auch Brandmeldeeinrichtungen basieren meist darauf, dass ein analoger Anschluss und/oder ISDN-Anschluss zur Verfügung steht. Diese Art der Anschlüsse kann meist von den IP-basierten Anlagen der Daten-Netzanbieter nicht zur Verfügung gestellt werden (oder nur über spezielle Adapter).

Die Verfügbarkeit von klassischen TK-Anlagen ist durch die innere Struktur der Anlagen viel höher als in Datennetz-Systemen. Was macht ein Datennetz-Administrator, wenn sein zentraler Switch ausgefallen ist? Er greift zum Telefon, um die Notfall-Hotline des Switch-Anbieters anzurufen. Das wird so dann in der reinen IP-Telefonie nicht mehr funktionieren. Auch bei der IP-Telefonie wird weiterhin der Übergang in das Öffentliche Fernsprechnetz benötigt und man muss damit auf die gute alte Technik zurückgreifen. Auch beginnen einige Netzanbieter z. Zt. Vorsorge zu treffen, dass ihre Netze nicht für VoIP zu nutzen sind (z. B. blockt O_2 VoIP auf ihren UMTS/GPRS-Flat-Rate-Verbindungen, Vodafone hat dies angekündigt).

Neue Telefonanlagen sollte man meiner Einschätzung nach, auch heutzutage, nur von den traditionellen Telekommunikationsfirmen wie z. B. Alcatel, Lucent, Nortel oder Siemens erwerben. Diese Anlagen sollten natürlich IP-fähig sein und in der Lage sein, die Systemapparate auch über Internetverbindungen betreiben zu können. SIP-Telefone sollten ebenso integrierbar sein. Dass die Strukturierte Verkabelung Grundlage der Sprachverbindungen sein muss, steht außer Frage. Bestehende Systeme sollten in dieser Beziehung modernisiert werden. Reine IP-Telefonsysteme sollten nicht eingesetzt werden, da sie nicht die gewohnte Qualität der Verfügbarkeit und Leistungsmerkmale bieten. Aus Sicherheitsgründen (und Verfügbarkeitsgründen) ist

es durchaus sinnvoll, zwei getrennte Systemwelten (Daten <-> Sprache) auch in einem Max-Planck-Institut zu betreiben.

Das Projekt „kopal“: Kooperativer Aufbau eines Langzeitarchivs digitaler Informationen

Dagmar Ullrich

Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

Einleitung

Ziel des kopal-Projekts[1] ist der Aufbau einer von Gedächtnisorganisationen, wie Bibliotheken, Archiven und Museen, nachnutzbaren technischen und organisatorischen Infrastruktur, die neben der Bewahrung digitaler Dokumente vor allem deren zukünftige Verfügbarkeit zum Ziel hat.

1. Projektpartner und Förderung

Das Projekt kopal wird in Zusammenarbeit der Deutschen Nationalbibliothek (DNB; vormals „Die Deutsche Bibliothek“), der Niedersächsischen Staats- und Universitätsbibliothek Göttingen (SUB), der Gesellschaft für

1. http://kopal.langzeitarchivierung.de [2006, 29. Mai]

wissenschaftliche Datenverarbeitung mbH Göttingen (GWDG) und der IBM Deutschland GmbH durchgeführt. Jeder der vier Partner des kopal-Projekts hat eigene Zuständigkeiten und Entwicklungsziele. Die beiden Bibliothekspartner DNB und SUB betreiben vorrangig die Entwicklungsarbeit für die bei ihnen vor Ort eingesetzten lokalen Softwaremodule. IBM arbeitet an der Weiterentwicklung der zentralen Software-Komponenten des Archivsystems. Die GWDG als Rechenzentrumspartner ist für den Betrieb des kopal-Systems, dessen Integration in die bestehende IT-Infrastruktur, die Netzanbindung, die Systemsicherheit, das System- und Datenbackup sowie für die Verwaltung der Speichermedien zuständig. Die Projektpartner arbeiten gemeinsam an der Entwicklung von Komponenten, die die langfristige Interpretierbarkeit der Archivinhalte sicherstellen sollen. Alle diese Aufgaben erfordern eine enge Zusammenarbeit und Koordination der beteiligten Partner. Die Gesamtprojektleitung liegt bei der DNB.

2. Projektförderung

Das Projekt kopal wird vom Bundesministerium für Bildung und Forschung (BMBF) über drei Jahre vom 01.07.2004 bis zum 30.06.2007 im Rahmen des Programms „IT-Forschung 2006“ mit einer Gesamtsumme von 4,2 Millionen Euro gefördert.[2]

3. Projektziele von kopal

Ein zentrales Projektziel von kopal ist die Konformität des Archivsystems mit **internationalen Standards**. Hierzu gehört an erster Stelle das OAIS-Referenzmodell[3] (Reference Model for an Open Archival Information System). Dieses Modell hat den Status eines ISO-Standards und beschreibt die in einem Archiv erforderlichen technischen und organisatorischen Einheiten und deren Zusammenspiel. Die in kopal verwendeten Metadaten der Archivobjekte entsprechen ebenfalls internationalen Standards bzw. basieren auf Ergebnissen internationaler Kooperationen. Zu diesen Metadaten-Standards gehören Dublin Core[4] (DC), Metadata Encoding & Transmission Stan-

2. http://www.bmbf.de/_media/press/akt_20040804-173.pdf [2006, 29. Mai]
3. Consultative Committee for Space Data Systems (CCSDS), Reference Model for an Open Archival Information System (OAIS), Washington DC, Januar 2002. Verfügbar: http://ssdoo.gsfc.nasa.gov/nost/wwwclassic/documents/pdf/CCSDS-650.0-B-1.pdf [2006, 29. Mai]
4. http://www.dublincore.org/ [2006, 29. Mai]

dard[5] (METS) und Langzeitarchivierungsmetadaten für elektronische Ressourcen[6] (LMER). Alle in das Archiv eingestellten Pakete verfügen darüber hinaus über einen dauerhaften Identifikationsmechanismus (Persistent Identifier). Hierfür verwendet kopal „Uniform Resource Names“ (URN)[7]. Die Einhaltung internationaler Standards und ein genau definiertes Eingabe- und Ausgabeformat für Datenpakete, dem „Universal Object Format“ (UOF), sollen einen **flexiblen Datenimport und -export** ermöglichen. Das Universelle Objektformat erlaubt es, **Materialien aller Art** zu speichern. Dabei kann es sich um digitale Dokumente der Formate PDF, TIFF oder TeX bis hin zu komplexen Objekten wie digitalen Videos handeln. Auch wenn nicht für alle diese Formate eine langfristige Interpretierbarkeit erreicht werden kann, so sollen doch zumindest der physische Erhalt und die Verwaltung beliebiger Datentypen innerhalb des kopal-Systems möglich sein. Um die künftige Interpretierbarkeit der archivierten Daten und damit ihre **Langzeitverfügbarkeit** zu gewährleisten, werden entsprechende Module entwickelt. Hierzu gehört u. a. ein „Monitoring-Tool“ zur rechtzeitigen Identifikation von Datenbeständen, deren Lesbarkeit absehbar gefährdet ist. Ebenfalls zu nennen sind hier die in Entwicklung befindlichen Komponenten zur automatisierten Durchführung von Erhaltungsstrategien wie Emulation oder Migration[8]. Grundlage aller dieser Archivierungsaktivitäten bildet die zuverlässige langfristige Speicherung der Datenobjekte selbst. Dieser Aufgabenbereich wird auch als „**Bitstream Preservation**“ bezeichnet. Um Datenverlust durch veraltete oder beschädigte Datenträger zu vermeiden, ist ein regelmäßiges Erneuern und Aktualisieren verwendeter Speichermedien und -techniken erforderlich. Die GWDG erstellt gemeinsam mit IBM ein Konzept für eine solche Medien-Erneuerung bzw. Aktualisierung. Das kopal-System erlaubt eine separate Nutzung durch verschiedene Institutionen (**Mandantenfähigkeit**). Vergleichbar getrennten Schließfächern, verfügt jede Institution über einen eigenen Bereich, in den nur sie Daten einstellen, verändern und abrufen kann. Die Institutionen können auch per

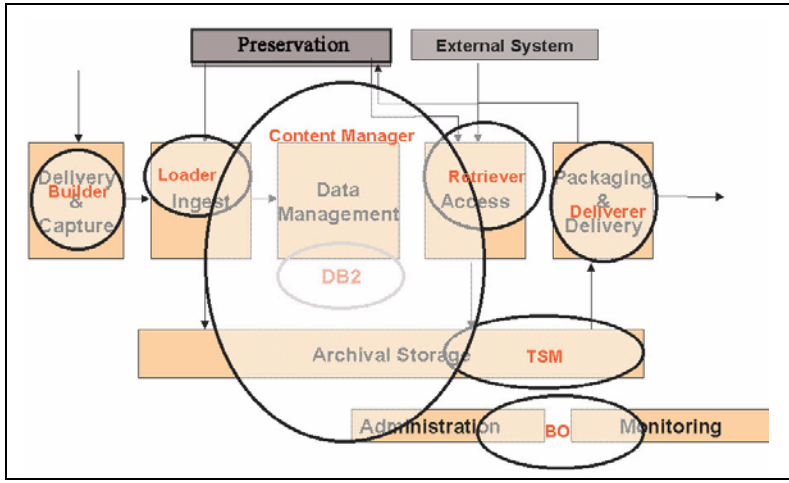
5. http://www.loc.gov/standards/mets/ [2006, 29. Mai]
6. http://www.ddb.de/standards/lmer/lmer.htm [2006, 29. Mai]
7. http://www.persistent-identifier.de/ [2006, 29. Mai], http://www.ietf.org/rfc/rfc2141.txt [2006, 29. Mai]
8. Eine Bestimmung dieser Begriffe findet sich in: Ullrich, Dagmar, Digitale Langzeitarchivierung. In: Generalverwaltung der Max-Planck-Gesellschaft (Hrsg.) : Max-Planck-Gesellschaft - Jahrbuch 2004. München : K. G. Saur, 2004, S. 785-789. - ISBN 3-927579-18-1, Kapitel 2.2.3.

Fernzugriff über sichere Internetverbindungen auf das kopal-System zugreifen. Die Mandantenfähigkeit und der mögliche Fernzugriff sind die Kernvoraussetzungen für die Nachnutzbarkeit des kopal-Systems durch andere Gedächtnisorganisationen. Für die zukünftige Akzeptanz wird aber auch die **transparente Integration** in vorhandene Informations- oder Bibliothekssysteme eine wesentliche Rolle spielen.

4. Technische Basis

4.1 Digital Information Archiving System (DIAS)[9]

Den Kern (**DIAS-Core**) der kopal-Solution bildet das von IBM in Zusammenarbeit mit der Koninklijke Bibliotheek (KB), der Nationalbibliothek der Niederlande, in Den Haag entwickelte Digital Information Archival System (DIAS). DIAS baut auf die IBM Standardsoftwarekomponenten DB2, Content Manager, Tivoli Storage Manager und Websphere Application Server auf. Sie werden durch DIAS-Module ergänzt. Die nachstehende Skizze[10] zeigt, welche Funktion die genannten Softwarekomponenten jeweils erfüllen.



9. http://www.ibm.com/nl/dias/ [2006, 29. Mai]

10. Grafik entnommen aus:
Van Diessen, Raymond J. und Steenbergen, Johan, The Long-Term Preservation Study of the DNEP Project - an Overview of the Results, Amsterdam, IBM Niederlande, Dezember 2002, IBM/KB Long-Term Preservation Study Report Series Number 1, Seite 6. Verfügbar: http://www.ibm.com/nl/dias/resource/overview.pdf [2006, 29. Mai]

DIAS-Core wurde für den Einsatz im kopal-Projekt erweitert. Bei diesen, bereits realisierten, Erweiterungen handelt es sich um die oben genannte Formatspezifikation der Eingabe- und Ausgabepakete (UOF), die auch die Standardisierung der Metadaten umfasst. Ebenfalls bereits realisiert wurden Mandantenfähigkeit und Fernzugriff auf das Archivsystem. Das an der KB entwickelte ursprüngliche DIAS war auf eine einzige Nutzerinstitution am gleichen Standort ausgerichtet. Dieser weiterentwickelte DIAS-Core wurde im Herbst 2005 bei der GWDG installiert.

4.2 koLibRI-Software[11]

Die beiden Bibliothekspartner DDB und SUB entwickeln im Projektzeitraum Softwaremodule, die vor Ort an den jeweiligen Institutionen eingesetzt werden. Diese Module der kopal Library for Retrieval and Ingest (koLibRI), dienen vorwiegend dem Zusammenstellen von Ein- und Ausgabepaketen entsprechend den Spezifikationen für das kopal-System sowie der Integration in die Informationssysteme vor Ort, wie z. B. dem Bibliotheks-OPAC. Die koLibRI-Software steht unter einer Open-Source-Lizenz und kann somit von anderen Organisationen jederzeit genutzt und an die eigenen Bedürfnisse angepasst werden.

5. Universelles Objektformat für kopal

Im Rahmen des Projektes wurde eine Spezifikation für Ein- und Ausgabeformat von Archivobjekten für das kopal-System entwickelt. Die oben bereits genannte Software koLibRI erstellt entsprechend dieser Spezifikation gepackte Archivdateien der Formate ZIP und TAR. Innerhalb der Pakete können sich beliebige Verzeichnisstrukturen mit je einer Metadaten-Datei (mets.xml) auf oberster Ebene befinden. In dem Paket kann jeder beliebige Dateityp enthalten sein. Für die Anzahl der Dateien gilt allerdings eine Obergrenze von 5.000. Die in das Archiv einzustellenden Pakete (SIP) sind bis auf eine interne ID, die erst vom Archivsystem vergeben wird, mit den späteren Ausgabepaketen (DIP) identisch. Eine ausführliche Darstellung des UOF findet sich auf den Projektwebseiten[12].

11. http://kopal.langzeitarchivierung.de/index_koLibRI.php.de [2006, 29. Mai]
12. http://kopal.langzeitarchivierung.de/downloads/kopal_Universelles_Objektformat.pdf [2006, 29. Mai]

6. Metadaten

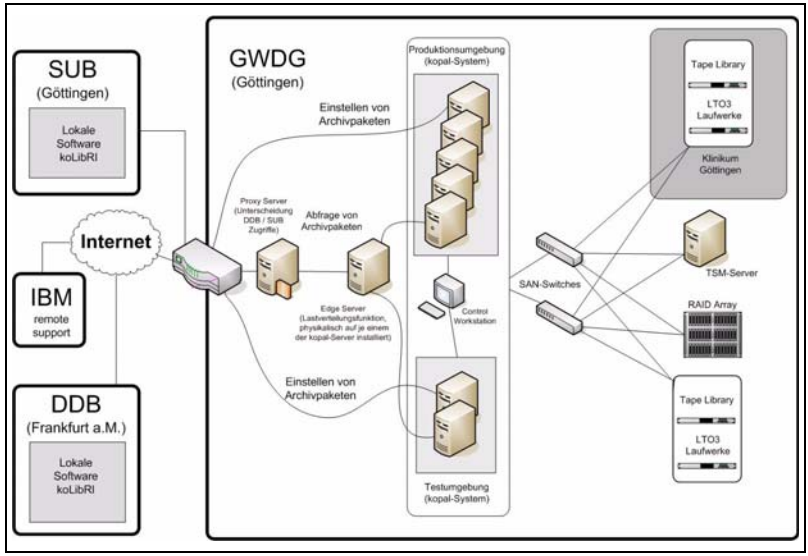
In der auf oberster Ebene liegenden XML-Datei sind alle Metadaten des Archivobjektes enthalten. Diese Metadatendateien entsprechen dem Metadata Encoding & Transmission Standard (METS). Bei METS handelt es sich um ein XML-Containerformat, das Abschnitte für beschreibende, administrative und strukturelle Metadaten enthält. Innerhalb des Abschnittes für die beschreibenden Metadaten kann das Dublin Core (DC) Metadatenformat genutzt werden. Die Metadaten enthalten auch speziell für die Langzeitarchivierung relevante Angaben, für deren Eintragung auf ein von der DDB entwickeltes Schema zurückgegriffen wird. Dieses Schema für „Langzeitarchivierungsmetadaten für elektronische Ressourcen“ (LMER) basiert auf einem Modell der Nationalbibliothek von Neuseeland[13].

Die in der mets.xml-Datei enthaltenen technischen Metadaten werden vom DIAS-Datenmodell erfasst und somit in der kopal-Datenbank gehalten. Sie bilden die Grundlage für künftige Migrations- und Emulationsstrategien. Die mets.xml-Dateien werden zusätzlich zu den Inhaltsdateien des Archivpakets gespeichert und können unabhängig abgefragt und ggf. mit anderen Archiven ausgetauscht werden.

13. http://www.natlib.govt.nz/en/whatsnew/4initiatives.html#meta [2006, 29. Mai]

7. Installation bei der GWDG

Die nachstehende Grafik zeigt die Infrastruktur des kopal-Projekts mit Fokus auf der Installation des Systems bei der GWDG.



Es handelt sich aktuell um sieben IBM-p550-Server mit je zwei 1,5-GHz-POWER5 Prozessoren und vier GByte SDRAM. Fünf dieser Server sind für den Einsatz im Produktivbetrieb vorgesehen, zwei dienen als Testumgebung. Zur Verwaltung des Systems wird eine Hardware-Management-Konsole (HMC) und eine Cluster-System-Management-Software (CSM) eingesetzt. Alle sieben Server sind an das Gigabit-Ethernet der GWDG angeschlossen und gegen unbefugten Zugriff von Außen mit entsprechenden Access Control Lists (ACLs) auf dem GWDG-Router gesichert. Ein Großteil der Zugriffe auf das System wird über einen vorgeschalteten Proxy-Server abgewickelt. Auf diesem Proxy-Server ordnet ein Webserver eingehende Anfragen den einzelnen Mandanten, DDB oder SUB, zu. Dann leitet er sie so an das System weiter, dass Zugriffe nur auf die jeweils institutseigenen Daten möglich sind. Die Anfragen werden dann vom Edge-Server entgegengenommen. Dieser Edge-Server erfüllt eine Lastverteilungsfunktion. Er verteilt die Anfragen auf die anderen Server und ermöglicht so eine optimale Ausnutzung der Systemkapazitäten. Physikalisch ist der Edge-Server auf je einem Produktiv- und einem Testserver installiert. Zur Sicherung gegen Stromausfälle ist das kopal-System an die Unterbrechungsfreie Stromversorgung (USV) der GWDG angeschlossen. Die von kopal genutzten Speichermedien

sind soweit möglich in das Storage Area Network (SAN) der GWDG integriert. Die derzeit von der GWDG vorangetriebene Speichervirtualisierung des SANs soll künftig auch dem kopal-System zugute kommen. Sowohl für die Speicherung von kopal-Archivpaketen als auch für das Backup des Systems werden die neuen Tape Libraries, zwei adic Scalar 10K mit LTO3-Laufwerken, eingesetzt. Wie bereits ihre Vorgänger befinden sich die Tape Libraries an zwei räumlich getrennten Standorten in Göttingen, eine direkt bei der GWDG, die zweite im Bereich Humanmedizin der Georg-August-Universität Göttingen, Geschäftsbereich Informationstechnologie. Neben diesen Bandmedien nutzt kopal ein IBM-DS4500-RAID-Array mit einer maximalen Ausbaustufe von 67 - 89 TByte je nach verwendetem Plattentyp. Dieses RAID-Array dient dem Betrieb der kopal-Software und als Speicher für Archivobjekte.

Bei der Wahl der Projekt-Hardware wurde besonders auf die spätere Skalierbarkeit geachtet, da im Rahmen eines Entwicklungsprojektes wie kopal eine genaue Spezifikation späterer Anforderungen zu Projektbeginn nur sehr eingeschränkt möglich ist.

8. DIAS User Group

Die kopal-Projektpartner DNB, SUB und GWDG haben sich mit der KB zur „DIAS User Group“ zusammengeschlossen. Ziel der „DIAS User Group“ ist es, gemeinsame Nutzerinteressen zu erkennen und bei der Weiterentwicklung von DIAS durch IBM zu vertreten. Darüber hinaus bietet der Zusammenschluss eine Plattform für Erfahrungsaustausch und gegenseitige Unterstützung. Die User Group ist offen für alle künftigen nachnutzenden Institutionen.

In der Reihe GWDG-Berichte sind zuletzt erschienen:

Nähere Informationen finden Sie im Internet unter
`http://www.gwdg.de/forschung/publikationen/gwdg-berichte`

Nr. 40 *Plesser, Theo und Peter Wittenburg* (Hrsg.):
Forschung und wissenschaftliches Rechnen - Beiträge zum Heinz-Billing-Preis 1994
1995

Nr. 41 *Brinkmeier, Fritz* (Hrsg.):
Rechner, Netze, Spezialisten. Vom Maschinenzentrum zum Kompetenzzentrum - Vorträge des Kolloquiums zum 25jährigen Bestehen der GWDG
1996

Nr. 42 *Plesser, Theo und Peter Wittenburg* (Hrsg.):
Forschung und wissenschaftliches Rechnen - Beiträge zum Heinz-Billing-Preis 1995
1996

Nr. 43 *Wall, Dieter* (Hrsg.):
Kostenrechnung im wissenschaftlichen Rechenzentrum - Das Göttinger Modell
1996

Nr. 44 *Plesser, Theo und Peter Wittenburg* (Hrsg.):
Forschung und wissenschaftliches Rechnen - Beiträge zum Heinz-Billing-Preis 1996
1997

Nr. 45 *Koke, Hartmut und Engelbert Ziegler* (Hrsg.):
13. DV-Treffen der Max-Planck-Institute - 21.-22. November 1996 in Göttingen
1997

Nr. 46 **Jahresberichte 1994 bis 1996**
1997

Nr. 47 *Heuer, Konrad, Eberhard Mönkeberg und Ulrich Schwardmann*:
Server-Betrieb mit Standard-PC-Hardware unter freien UNIX-Betriebssystemen
1998

Nr. 48 *Haan, Oswald* (Hrsg.):
Göttinger Informatik Kolloquium - Vorträge aus den Jahren 1996/97
1998

Nr. 49 *Koke, Hartmut und Engelbert Ziegler* (Hrsg.):
IT-Infrastruktur im wissenschaftlichen Umfeld - 14. DV-Treffen der Max-Planck-Institute, 20. - 21. November 1997 in Göttingen
1998

Nr. 50 *Gerling, Rainer W.* (Hrsg.):
Datenschutz und neue Medien - Datenschutzschulung am 25./26. Mai 1998
1998

Nr. 51 *Plesser, Theo und Peter Wittenburg* (Hrsg.):
Forschung und wissenschaftliches Rechnen - Beiträge zum Heinz-Billing-Preis 1997
1998

Nr. 52 *Heinzel, Stefan und Theo Plesser* (Hrsg.):
Forschung und wissenschaftliches Rechnen - Beiträge zum Heinz-Billing-Preis 1998
1999

Nr. 53 *Kaspar, Friedbert und Hans-Ulrich Zimmermann* (Hrsg.):
Internet- und Intranet-Technologien in der wissenschaftlichen Datenverarbeitung - 15. DV-Treffen der Max-Planck-Institute, 18. - 20. November 1998 in Göttingen
1999

Nr. 54 *Plesser, Theo und Helmut Hayd* (Hrsg.):
Forschung und wissenschaftliches Rechnen - Beiträge zum Heinz-Billing-Preis 1999
2000

Nr. 55 *Kaspar, Friedbert und Hans-Ulrich Zimmermann* (Hrsg.):
Neue Technologien zur Nutzung von Netzdiensten - 16. DV-Treffen der Max-Planck-Institute, 17. - 19. November 1999 in Göttingen
2000

Nr. 56 *Plesser, Theo und Helmut Hayd* (Hrsg.):
Forschung und wissenschaftliches Rechnen - Beiträge zum Heinz-Billing-Preis 2000
2001

Nr. 57 *Hayd, Helmut und Rainer Kleinrensing* (Hrsg.):
17. und 18. DV-Treffen der Max-Planck-Institute
22. - 24. November 2000 in Göttingen
21. - 23. November 2001 in Göttingen
2002

Nr. 58 *Plesser, Theo und Volker Macho* (Hrsg.):
Forschung und wissenschaftliches Rechnen - Beiträge zum Heinz-Billing-Preis 2001
2003

Nr. 59 *Suchodoletz, Dirk von*:
Effizienter Betrieb großer Rechnerpools - Implementierung am Beispiel des Studierendennetzes an der Universität Göttingen
2003

Nr. 60 *Haan, Oswald* (Hrsg.):
Erfahrungen mit den IBM-Parallelrechnersystemen RS/6000 SP und pSeries690
2003

Nr. 61 *Rieger, Sebastian:*
Streaming-Media und Multicasting in drahtlosen Netzwerken - Untersuchung von Realisierungs- und Anwendungsmöglichkeiten
2003

Nr. 62 *Kremer, Kurt und Volker Macho* (Hrsg.):
Forschung und wissenschaftliches Rechnen - Beiträge zum Heinz-Billing-Preis 2002
2003

Nr. 63 *Kremer, Kurt und Volker Macho* (Hrsg.):
Forschung und wissenschaftliches Rechnen - Beiträge zum Heinz-Billing-Preis 2003
2004

Nr. 64 *Koke, Hartmut* (Hrsg.):
GÖ* – Integriertes Informationsmanagement im heterogenen eScience-Umfeld: GÖ*-Vorantrag für die DFG-Förderinitiative „Leistungszentren für Forschungsinformation“
2004

Nr. 65 *Koke, Hartmut* (Hrsg.):
GÖ* – Integriertes Informationsmanagement im heterogenen eScience-Umfeld: GÖ*-Hauptantrag für die DFG-Förderinitiative „Leistungszentren für Forschungsinformation“
2004

Nr. 66 *Bussmann, Dietmar und Andreas Oberreuter* (Hrsg.):
19. und 20. DV-Treffen der Max-Planck-Institute
20. - 22. November 2002 in Göttingen
19. - 21. November 2003 in Göttingen
2004

Nr. 67 *Gartmann, Christoph und Jochen Jähnke* (Hrsg.):
21. DV-Treffen der Max-Planck-Institute
17. - 19. November 2004 in Göttingen
2005

Nr. 68 *Kremer, Kurt und Volker Macho* (Hrsg.):
Forschung und wissenschaftliches Rechnen - Beiträge zum Heinz-Billing-Preis 2004
2005

Nr. 69 *Kremer, Kurt und Volker Macho* (Hrsg.):
Forschung und wissenschaftliches Rechnen - Beiträge zum Heinz-Billing-Preis 2005
2006

Nr. 70 *Gartmann, Christoph und Jochen Jähnke* (Hrsg.):
22. DV-Treffen der Max-Planck-Institute
16. - 18. November 2005 in Göttingen
2006