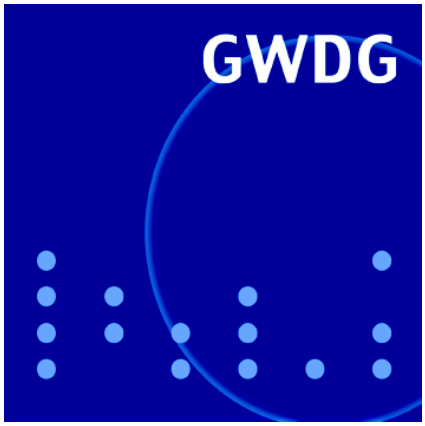

Umbauarbeiten

Batch-System LSF

IT-Sicherheitsleitlinie

Videokonferenzdienst DFNVC

GWDG Nachrichten

6 / 2004

Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

Inhaltsverzeichnis

1. Umbauarbeiten im Rechenzentrum und Konsequenzen für Benutzer 3

2. Kontingentzuweisung für das dritte Quartal 2004 3

3. Informationsveranstaltung „Sicherheit im GÖNET“ am 29.06.2004 4

4. Einheitliches Batch-System LSF 4

5. IT-Sicherheitsleitlinie der GWDG 9

6. Der Videokonferenzdienst des DFN-Vereins und seine Nutzung über den Gatekeeper der GWDG 13

7. Kurse des Rechenzentrums 18

8. Betriebsstatistik Mai 2004 24

9. Autoren dieser Ausgabe 24

GWDG-Nachrichten für die Benutzer des Rechenzentrums

ISSN 0940-4686

27. Jahrgang, Ausgabe 6 / 2004

http://www.gwdg.de/GWDG-Nachrichten

Herausgeber: Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen
Am Faßberg, 37077 Göttingen-Nikolausberg

Redaktion: Dr. Th. Otto Tel.: 0551 201-1828, E-Mail: Thomas.Otto@gwdg.de
Herstellung: S. Greber Tel.: 0551 201-1518, E-Mail: Sigrun.Greber@gwdg.de

1. Umbauarbeiten im Rechenzentrum und Konsequenzen für Benutzer

Die Anwender, die die Rechenanlagen und Netze vor Ort, also im Rechenzentrum auf dem Fassberg nutzen, haben es bereits seit einiger Zeit mitbekommen: Es ist eine gewisse Unruhe in den Benutzerräumen eingezogen! Die Ursache dafür sind Umbauarbeiten, die mittlerweile erforderlich wurden, um dem gestiegenen Platzbedarf der demnächst aufzustellenden neuen Geräte Rechnung zu tragen. Die Umbauarbeiten sehen vor, dass im bisherigen Dialoggeräteraum bis auf drei Schwarzweiß-Drucker alle Peripheriegeräte untergebracht werden. Die Bildschirmarbeitsplätze aus diesem Raum werden in den frei werdenden Bereichen aufgestellt. Die Zahl der Arbeitsplätze im Rechenzentrum wird sich dadurch nicht verändern.

Für die Anwender bedeutet das, sich an neue Räumlichkeiten zu gewöhnen. Die Unannehmlichkeiten, die durch die Umräumaktion hervorgerufen werden, bitten wir zu entschuldigen. Wir hoffen, dass die diesbezüglichen Arbeiten Ende Juni abgeschlossen sein werden.

Durch die Zusammenlegung der Peripherie in einen Raum lassen sich die Geräte intensiver als bisher bei der verteilten Aufstellung überwachen. Fehlersituationen sind dadurch schneller erkennbar und damit auch schneller behebbar. Wir hoffen, durch die Konzentration der Geräte den Benutzern einen verbesserten Service anbieten zu können.

Grieger

---

2. Kontingentzuweisung für das dritte Quartal 2004

Die nächste Zuweisung von Institutskontingenten für die Inanspruchnahme von Leistungen der GWDG erfolgt am Donnerstag, dem 1. Juli 2004. Die Höhe der Kontingente wird den Instituten per Brief oder per E-Mail mitgeteilt. Die Bemessung der Institutskontingente erfolgte nach den Vorläufigen Richtlinien des Beirats der GWDG und den Ergänzungen der Beiratskommission für die Verteilung von Rechenleistung entsprechend dem Verbrauch im Zeitraum vom 1.12.2003 bis 31.5.2004. Nicht verbrauchte Kontingente werden zu 50 % in das nächste Quartal übertragen. Negative Verbrauchswerte werden zu 100 % mit dem neuen Institutskontingent verrechnet.

Jeder Benutzer kann den aktuellen Stand des Institutskontingents durch die Eingabe des Kommandos

```
kontingent
```

auf einer Workstation des UNIX-Clusters oder im WWW unter dem URL

```
http://www.gwdg.de/service/nutzung/
                              kontingentierung
```

abfragen. Dort besteht auch die Möglichkeit, Informationen über den Stand des separaten Druckkontingents abzurufen.

Falls in Ausnahmefällen das Institutskontingent nicht ausreichen sollte, können schriftlich begründete Anträge an die Beiratskommission für die Verteilung von Rechenleistung gestellt werden. Solche Anträge sollen bis zum 23.8.2004 im Rechenzentrum eingereicht werden; Vordrucke und Hinweise dazu sind sowohl bei der Information als auch im WWW unter dem URL

```
http://www.gwdg.de/service/nutzung/
                              antragsformulare
```

erhältlich. Da aber die Bearbeitung der Anträge mittlerweile **vollständig elektronisch** erfolgt, ist die Übersendung der Anträge mit Begründung per E-Mail an die Adressen wgriege@gwdg.de oder gwdg@gwdg.de **erwünscht**.

Grieger

3. Informationsveranstaltung „Sicherheit im GÖNET“ am 29.06.2004

Im Dezember 2003 hatte die GWDG alle System- und Netzbetreuer im GÖNET eingeladen, um über die Sicherheit im GÖNET zu informieren und zu diskutieren. Die Teilnehmer äußerten den Wunsch, solche Veranstaltungen regelmäßig zu wiederholen.

Diesem Wunsch will die GWDG gern entsprechen und lädt daher zu einem erneuten Treffen ein.

Termin: Dienstag, 29.06.2004, um 14.00 Uhr

Dauer: ca. 2 Stunden

Ort: Hörsaal des MPI für biophysikalische Chemie, Göttingen, Am Faßberg

Diese Veranstaltung richtet sich an die Rechner- und Netzwerkbetreuer der am GÖNET angeschlossenen Institute. Auch diesmal wird die GWDG zunächst über die aktuelle Lage und zukünftige Planungen berichten. Anregungen aus dem Nutzerkreis für die Gestaltung des Treffen sind auch im Vorfeld erwünscht (z. B. per E-Mail an Holger.Beck@gwdg.de).

Weitere Informationen zur Veranstaltung werden zeitnah über die GÖNET-Mailing-Liste und im WWW unter

`http://www.gwdg.de/forschung/veranstaltungen/workshops`

zur Verfügung gestellt.

Wir hoffen wiederum auf eine lebhafte Diskussion und eine ebenso rege Beteiligung wie im Dezember.

Beck

---

4. Einheitliches Batch-System LSF

4.1 Einleitung

Die GWDG stellt Rechenleistung auf unterschiedlichen Hardware-Plattformen zur Verfügung. Für die Verwaltung von Benutzeraufträgen für die verschiedenen Rechnersysteme wurden im Laufe der Jahre drei Batch-Systemene eingesetzt: **Codine** für sequentielle Anwendungen, **LoadLeveler** für parallele Anwendungen auf den IBM-Parallelrechnern und **LSF** (Load Sharing Facility) für parallele und sequentielle Anwendungen auf dem Linux-Cluster. Die Verwendung unterschiedlicher Batch-Verwaltungssysteme bedeuteten für Betreuer und Nutzer der Rechenanlagen einen hohen Aufwand.

Die GWDG hat nun mit der Firma *Platform Computing* einen Lizenzvertrag zum Einsatz von LSF auf allen Rechnersystemen der GWDG abgschlossen. Damit können Codine und LoadLeveler durch LSF ersetzt werden. Die Umstellung auf LSF ist für alle Rechnersysteme technisch vorbereitet worden. Nun soll in einem dreiphasigen Umstellungsprozess der Übergang von Codine und LoadLeveler auf LSF durchgeführt werden:

1. Seit Donnerstag, dem 27.05.2004, sind LSF-Queues für die Nutzung von Ressourcen auf der IBM RS/6000 SP, IBM pSeries690 und den Kursraumrechnern aktiviert. Die LSF-Queues verwalten zunächst nur einen kleinen Teil der Ressourcen der IBM-Systeme (acht Knoten der RS/6000 SP, ein Knoten der pSeries690). Damit soll den Benutzern die Gelegenheit gegeben werden, ihre Job-Skripten auf die Verwendung von LSF umzustellen und in geringem Umfang den Produktionsbetrieb unter LSF aufzunehmen. Diese Phase wird vier Wochen, also bis zum 23.06.2004 dauern.
2. Ab dem 24.06.2004 wird dann etwa die Hälfte der IBM-Rechenleistung unter LSF-Verwaltung gestellt, so dass Nutzer, die ihre Job-Skripten umgestellt haben, nun ganz unter LSF rechnen können. Die Dauer dieser Phase hängt davon ab, wie schnell die übrigen Nutzer nach LSF migrieren können. Da die Aufspaltung der Ressourcen auf mehrere Batch-Systeme die Auslastung behindert, sollte diese Phase möglichst schnell, längstens nach weiteren vier Wochen beendet werden.
3. Danach werden alle Rechnerressourcen der GWDG (mit Ausnahme der DEC-Syteme) einheitlich über LSF verwaltet.

Die Dokumentation zur Nutzung von LSF auf den Rechnern der GWDG ist auf den Web-Seiten der GWDG unter dem URL

`http://www.gwdg.de/service/rechenanlagen/lsf`

zu finden.

Bei Fragen zu LSF und zur Umstellung Ihrer Job-Skripten wenden Sie sich bitte an Herrn Dr. Christian Boehme (E-Mail: cboehme1@gwdg.de).

4.2 Übersicht

Das Batch-System Load Sharing Facility (LSF) der Firma Platform erlaubt es, alle Batch-Rechenressourcen der GWDG mit den gleichen Kommandos zu benutzen. Der Zugriff auf LSF kann von allen Rechnern aus erfolgen, auf denen bisher der Zugriff auf die Batch-Systeme LSF, Codine oder den IBM LoadLeveler möglich war. Dazu gehören die **`gwdu102`**, die **`gwdk032`** und die **`gwdk081`**. LSF ist so konfiguriert, dass die verschiedenen bei der GWDG zur Verfügung stehenden Rechnerarchitekturen eigenen Warteschlangen („queues“) zugeordnet sind. Spezielle Anforderungen wie größerer temporärer Plattenplatz oder mehr Hauptspeicher werden dagegen nicht über queues geregelt, sondern müssen vom Benutzer bei der Submittierung eines Jobs spezifiziert werden. Die zu einer Architektur gehörigen Rechner („hosts“) sind außerdem zu Gruppen („hostgroups“) zusammengefasst, wobei es zusätzliche Untergruppen von hosts mit besonderen Ressourcen gibt. Eine Übersicht über die LSF-Konfiguration gibt die folgende Tabelle. **Während einer Übergangszeit stehen zunächst nicht alle aufgeführten Systeme unter LSF zur Verfügung.**

LSF - Konfiguration

Queue	System	Hostgroup	Spezielle Ressource	Vorhanden	Anzahl Slots	Maximale Walltime (Stunden)
gwdg-pcpar	Linux-Cluster	hgrouppcpar			198	48
gwdg-pcser	Linux-Workstations	hgrouppcser	Modell	P4-1700 MHz (Minimum)	24	48
		hgrouppcser-fst		Xeon-3060 MHz	8	
gwdg-rs6k(-long)	IBM RS/6000 SP	hgrouprs6k	Scratch	9 GB (Minimum)	116 (32)	48 (96*)
		hgrouprs6k-scr		16 GB	20	
		gwdk031		72 GB	4	
gwdg-p690	IBM pSeries690	hgroupp690	Hauptspeicher/ Modell	32 GB/1100 MHz (Minimum)	128	24
		gwdk081		64 GB/1100 MHz	32	
		gwdk084		32 GB/1700 MHz	32	

** Die maximale Aufenthaltszeit („walltime“) ist unlimitiert, die maximale CPU-Zeit beträgt 96 Stunden. gwdg-rs6k-long ist daher für Jobs mit schwer vorhersagbarer walltime geeignet.*

Die hier vorliegende Dokumentation erklärt nur die für GWDG-Nutzer wichtigsten Aspekte von LSF sowie die speziellen Eigenschaften der GWDG-Konfiguration. Weitere Informationen finden Sie in der englischen Nutzerdokumentation sowie in den manpages.

4.3 Kommandos

4.3.1 Jobs submittieren: bsub

1. Syntax

```
bsub -q queuename -a wrapper -n nproc
-W hh:mm -m host -R resourcestring
jobcommand
bsub < jobscript
```

2. Erläuterungen

Mit **`bsub`** können Jobs an LSF übergeben werden. Optionen können als Teil der Kommandozeile eingegeben werden oder in einer Skriptdatei im Anschluss an die Auswahl der shell enthalten sein, wobei jeder Option ein **`#BSUB`** vorangestellt wird (siehe Beispiele). Die wichtigsten Optionen sind:

`-q` ***`queuename`***

Mögliche Queue-Namen können Sie der Übersichtstabelle entnehmen. Mit der queue wird entsprechend dieser Tabelle auch die Architektur ausgewählt. Die queue **`gwdg-rs6k-long`** ist für lange Jobs mit schwer vorhersagbaren absoluten Laufzeiten gedacht. Hier ist die verbrauchte CPU-Zeit, nicht aber die walltime beschränkt.

`-a` ***`wrapper`***

Wrapper sind vorkonfigurierte Skripten, die die Submittierung von Paralleljobs erleichtern. Zur Zeit stehen folgende wrapper zur Verfügung:

- **`openmp`** für SMP-Jobs in den queues **`gwdg-pcpar`**, **`gwdg-rs6k`** und **`gwdg-p690`**
- **`scampi`** für MPI-Jobs in queue **`gwdg-pcpar`**
- **`hyb-pcpar`** für SMP/MPI-Hybridjobs in queue **`gwdg-pcpar`**

- **poe-rs6k** für MPI-Jobs in queue **gwdg-rs6k**
- **poe-p690** für MPI-Jobs in queue **gwdg-p690**

Wenn vor dem eigentlichen MPI-Programm in einem Jobskript serielle Befehle abgearbeitet werden sollen, muss statt der **-a**-Option direkt **pam** aufgerufen werden (siehe Beispiele):

- **pam -g sca_mpimon_wrapper** für MPI-Jobs in queue **gwdg-pcpar**
- **pam -g sca_mpimon_hybridwrapper** für SMP/MPI-Hybridjobs in queue **gwdg-pcpar**
- **pam -g 1 poe-rs6k** für MPI-Jobs in queue **gwdg-rs6k**
- **pam -g 1 poe-p690** für MPI-Jobs in queue **gwdg-p690**

-n *nproc*

Mit dieser Option wird die Zahl der Prozessoren angegeben. Beachten Sie bitte, dass jetzt auch für SMP- und Hybridjobs die Gesamtzahl der verwendeten Prozessoren angegeben werden muss.

-W *hh:mm*

Hiermit wird die walltime, also die maximale Verweildauer im Status „run“ des Jobs, in Stunden und Minuten festgelegt. Höchstwerte für die jeweiligen queues finden Sie in der Übersichtstabelle.

-m *host*

Hiermit können zulässige hosts für den Job definiert werden. Dies ist notwendig, wenn der Job spezielle Ressourcenanforderungen hat, die nicht von allen hosts einer Architektur gleich gut erfüllt werden können. Mehrere hosts werden in Anführungszeichen durch Leerzeichen getrennt angegeben (host1 host2 host3). Anstelle von Host-Namen können auch hostgroups aus der Übersichtstabelle verwendet werden. Wichtige Anwendungsfälle für diese Option sind:

- Für mehr als 2 GB scratch pro Prozessor in gwdg-rs6k **-m hgrouprs6k-scr**
- Für mehr als 4 GB scratch pro Prozessor in gwdg-rs6k **-m gwdk031**
- Für mehr als 1 GB Hauptspeicher pro Prozessor in gwdg-p690 **-m gwdk081**

Hosts und hostgroups für schnellere Prozessoren innerhalb einer Architektur sind ebenfalls in der Übersichtstabelle aufgeführt, diese können aber auch über die Angabe des Modells im resourcestring (s. u.) spezifiziert werden.

-R *resourcestring*

Der resourcestring erlaubt die Zuteilung spezieller Ressourcen für den Job. Mehrere Ressourcenanforderungen werden in Anführungszeichen gefasst und durch Leerzeichen getrennt. Jede Anforderung hat die Syntax ***section[string]***. **section** kann eines der Schlüsselwörter **select**, **order**, **rusage**, **span** und **same** sein. Mögliche Anwendungen für die GWDG-Konfiguration sind:

select

Mittels des selectstrings kann in den queues **gwdg-pcser** (**select[model=PC3060]**) und **gwdg-p690** (**select[model=Power417]**)eine schnellere CPU angefordert werden.

rusage

In der queue **gwdg-rs6k** wird mit **rusage[resscr=*sizeofscratch*]** temporärer Plattenplatz reserviert. Die Angabe erfolgt in MegaByte und pro Prozessor. Bitte beachten Sie, dass bei mehr als 2000 MB pro Prozessor die hostgroup **hgrouprs6k-scr**, bei mehr als 4000 MB der host **gwdk031** angefordert werden muss (siehe **-m**-Option). Analog können in der queue **gwdg-p690** mit **rusage[resmem=*sizeofmem*]** sizeofmem MB Hauptspeicher pro Prozessor angefordert werden. Hier muss bei mehr als 1000 MB pro Prozessor der host **gwdk081** verwendet werden.

span

Mit **span[ptile=*npn*]** werden die insgesamt angeforderten Prozessoren in Blöcken der Größe **npn** auf die ausführenden hosts verteilt. Wenn alle Prozesse auf dem gleichen host alloziert werden sollen, muss **npn** gleich **nproc** (siehe **-n**-Option) gewählt werden. Für die exklusive Nutzung eines hosts muss **npn** gleich der Zahl der auf dem host verfügbaren Prozessoren sein. Die exklusive Nutzung eines hosts mittels des **-x**-Schalters wird nicht mehr unterstützt.

3. Beispiele

Jobs auf dem Linux-Cluster (queue gwdg-pcpar)

1. Anforderung von 24 h auf einer CPU für das Programm **serprog**:

   ```
   bsub -q gwdg-pcpar -W 24:00 serprog
   ```

2. Exklusive Nutzung eines hosts, seriell oder SMP-parallelisiert. Der wrapper **openmp** (**-a**-Option) sorgt dafür, dass das Programm nur einmal gestartet wird. **-R span[ptile=2]** alloziert beide Prozessoren (**-n 2**) auf demselben host. Für ein SMP-Programm, z. B. Gaussian im Parallelmodus, ist der Aufruf identisch:

   ```
   bsub -q gwdg-pcpar -W 24:00 -a openmp
   -n 2 -R span[ptile=2] serprog
   ```

3. Anforderung von 24 h auf 32 Prozessoren für das MPI-Programm **mpiprog**. Beim Starten wird der MPI-wrapper **scampi** verwendet:

   ```
   bsub -q gwdg-pcpar -W 24:00 -a scampi
   -n 32 mpiprog
   ```

4. Wie 3., aber mit einem Jobskript **jobscript**:

   ```
   bsub < jobscript
   ```

   Das Jobskript **jobscript** enthält:

   ```
   #!/bin/sh
   #BSUB -q gwdg-pcpar
   #BSUB -W 24:00
   #BSUB -n 32
   pam -g sca_mpimon_wrapper mpiprog
   ```

Jobs auf der IBM pSeries690 (queue gwdg-p690)

1. Anforderung von 24 h auf einer CPU mit 1 GB Hauptspeicher (**rusage[resmem=1000])** für das Programm **serprog**. Der benötigte Hauptspeicher muss in queue **gwdg-p690** immer angegeben werden.

   ```
   bsub -q gwdg-p690 -W 24:00 -R
   rusage[resmem=1000] serprog
   ```

2. Anforderung von 24 h auf 16 Prozessoren (**-n 16)** mit 1 GB Hauptspeicher pro Prozessor, also 16 GB Hauptspeicher insgesamt, für das SMP-Programm **smpprog**. **-a openmp** verwendet den openmp-wrapper zum Starten des Programms. Er ist auch für nicht mit OpenMP parallelisierte SMP-Programme geeignet:

   ```
   bsub -q gwdg-p690 -W 24:00 -a openmp
   -n 16 -R rusage[resmem=1000] smpprog
   ```

3. Wie 2., aber mit 2 GB Hauptspeicher pro Prozessor. Bei mehr als 1 GB pro Prozessor muss die **gwdk081** verwendet werden (**-m**-Option):

   ```
   bsub -q gwdg-p690 -W 24:00 -m gwdk081
   -a openmp -n 16 -R rusage[resmem=2000]
   smpprog
   ```

4. Wie 3., aber mit einem Jobskript **jobscript**:

   ```
   bsub < jobscript
   ```

   Das Jobskript **jobscript** enthält:

   ```
   #!/bin/sh
   #BSUB -q gwdg-p690
   #BSUB -W 24:00
   #BSUB -m gwdk081
   #BSUB -a openmp
   #BSUB -n 16
   #BSUB -R rusage[resmem=2000]
   smpprog
   ```

5. Start eines MPI-Programms auf 16 Prozessoren. Hier wird der poe-wrapper **poe-p690** verwendet, der auch die passende queue wählt. Die Optionen nach dem Programmnamen **mpiprog** (und möglichen, hier nicht vorhandenen Programmoptionen) werden an **poe** übergeben. Die **poe**-Option **-shared_memory yes** wählt die schnelle shared-memory-Kommunikation für Prozesse auf dem gleichen host:

   ```
   bsub -a poe-p690 -n 16 -R rusage[res-
   mem=500] mpiprog -shared_memory yes
   ```

6. Wie 5., aber mit einem Jobskript **jobscript**:

   ```
   bsub < jobscript
   ```

   Das Jobskript **jobscript** enthält:

   ```
   #!/bin/sh
   #BSUB -q gwdg-p690
   #BSUB -n 16
   #BSUB -R rusage[resmem=500]
   pam -g 1 poe-p690 mpiprog -
   shared_memory yes
   ```

Jobs auf der IBM RS/6000 SP (queue gwdg-rs6k)

1. Anforderung von 24 h auf einer CPU für das Programm **serprog**:

   ```
   bsub -q gwdg-rs6k -W 24:00 serprog
   ```

2. Anforderung von 24 h mit 2 GB temporärem Plattenplatz (**-R rusage[resscr=2000]**) für das Programm **serprog**:

   ```
   bsub -q gwdg-rs6k -W 24:00 -R
   rusage[resscr=2000] serprog
   ```

3. Wie 2., aber mit 3 GB temporärem Plattenplatz. Bei mehr als 2 GB pro Prozessor muss die hostgroup **hgrouprs6k-scr** verwendet werden (**-m**-Option):

   ```
   bsub -q gwdg-rs6k -W 24:00 -m
   hgrouprs6k-scr -R rusage[resscr=3000]
   serprog
   ```

4. Wie 2., aber für ein SMP-Programm **smpprog** auf vier Prozessoren (**-n 4**). Insgesamt werden hier 8 GB temporärer Plattenplatz reserviert. **-a openmp** sorgt dafür, dass der SMP-wrapper **openmp** beim Programmstart verwendet wird. **span[ptile=4]** alloziert alle vier Prozessoren auf demselben host:

   ```
   bsub -q gwdg-rs6k -W 24:00 -a openmp -n
   4 -R "rusage[resscr=2000]
   span[ptile=4]" smpprog
   ```

5. Start eines MPI-Programms auf 16 Prozessoren. Hier wird der poe-wrapper **poe-rs6k** verwendet, der auch die passende queue wählt. Die Optionen nach dem Programmnamen **mpiprog** (und möglichen, hier nicht vorhandenen Programmoptionen) werden an **poe** übergeben. Die **poe**-Option **-euilib us** wählt den IBM-high-performance-switch für die Kommunikation zwischen den hosts, **-shared_memory yes** die schnelle shared-memory-Kommunikation für Prozesse auf dem gleichen host. Die beiden

Optionen müssen in der im Beispiel angegebenen Reihenfolge verwendet werden:

```
bsub -a poe-rs6k -n 16 mpiprog
-shared_memory yes -euilib us
```

6. Wie 5., aber mit einem Jobskript **jobscript**:

   ```
   bsub < jobscript
   ```

   Das Jobskript **jobscript** enthält:

   ```
   #!/bin/sh
   #BSUB -q gwdg-rs6k
   #BSUB -n 16
   pam -g 1 poe-rs6k mpiprog
   -shared_memory yes -euilib us
   ```

7. Ein Gaussian03-Job auf einem Prozessor mit 2 GB scratch kann mittels des Skripts **g03lsf** submittiert werden:

   ```
   bsub < g03lsf
   ```

   g03lsf enthält:

   ```
   #!/bin/ksh
   #BSUB -q gwdg-rs6k
   #BSUB -W 48:00
   #BSUB -R rusage[resscr=2000]
   export g03root="/usr/product/gaussian"
   . $g03root/g03/bsd/g03.profile
   export GAUSS_SCRDIR="/scratch"
   g03 < input.com > output.log
   ```

4.3.2 Jobs beobachten: bjobs

1. Syntax

```
bjobs -l -a -r -p -u uid -m host jobid
```

2. Erläuterungen

Mit **bjobs** kann der Status eines Jobs angezeigt werden. Wenn keine **jobid** angegeben wird, werden alle mit den gewählten Optionen übereinstimmenden Jobs angezeigt.

-l

Zeigt die ausführliche Statusbeschreibung eines Jobs.

-a -r -p

-a zeigt laufende (RUN), wartende (PEND) und kürzlich beendete Jobs an. Standardmäßig werden nur laufende und wartende Jobs angezeigt. **-r** zeigt nur laufende, **-p** nur wartende Jobs.

-u *uid*

Es werden die Jobs von Nutzer **uid** angezeigt. Ohne Angabe werden die eigenen Jobs angezeigt. Mit **uid=all** werden die Jobs aller Nutzer angezeigt.

-m *host*

Es werden nur Jobs angezeigt, die auf den angegebenen hosts oder der hostgroup laufen. Mehrere hosts oder hostgroups werden durch Leerzeichen getrennt in Anführungszeichen angegeben (z. B. **-m "gwdl001 hgrouppcser"**)

3. Beispiel

Anzeigen aller laufenden Jobs von Nutzer cboehme1 auf der IBM RS/6000 SP

```
bjobs -r -u cboehme1 -m hgrouprs6k
```

4.3.3 Jobs beenden: bkill

1. Syntax

```
bkill -r -u uid -m host -q queue jobid
```

2. Erläuterungen

Mit **bkill** kann ein laufender Job abgebrochen oder ein wartender Job aus der Warteschlange entfernt werden. Wenn keine **jobid** angegeben wird, muss eine der Optionen **-u -m -q** verwendet werden. Betroffen ist dann der letzte Job, auf den die angegebenen Kriterien zutreffen. Die Angabe von **jobid=0** führt zur Anwendung auf alle Jobs, die den jeweiligen Kriterien entsprechen.

-r

Entfernt einen Job aus der Warteschlange, ohne auf die Bestätigung des Betriebssystems zu warten, dass der Job beendet ist. Nur für Fälle, in denen ein Job anders nicht zu entfernen ist.

-u *uid* -m *host* -q *queue*

Mit diesen Optionen werden Kriterien festgelegt, nach denen **bkill** auf Jobs angewendet wird. **-u uid** betrifft Jobs des Nutzers **uid** (nur Administratoren können Jobs anderer Nutzer entfernen), **-m host** Jobs auf dem angegebenen host oder der hostgroup und **-q queue** Jobs der angegebenen queue. Ohne Angabe einer **jobid** wirkt **bkill** auf den letzten, mit **jobid=0** auf alle passenden Jobs. Bei allen anderen Angaben für **jobid** sind diese Optionen wirkungslos.

3. Beispiele

1. Entfernen des Jobs 14444:

   ```
   bkill 14444
   ```

2. Entfernen aller Jobs in der queue *gwdg-pcser*, die auf host **gwdl111** laufen:

   ```
   bkill -m gwdl111 -q gwdg-pcser 0
   ```

4.3.4 Informationen über hosts: bhosts

1. Syntax

```
bhosts -l -w host
```

2. Erläuterungen

Mit **bhosts** werden Informationen über den host oder die hostgroup **host** abgefragt.

-l -w

-l und **-w** steuern die Ausgabe. **-w** erzeugt eine gegenüber dem Standard etwas erweiterte Ausgabe, bleibt aber bei einer Zeile pro host. **-l** ergibt eine ausführliche mehrzeilige Ausgabe pro host.

3. Beispiele

1. Erweiterte Einzeilendarstellung aller hosts

   bhosts -w

2. Ausführliche Mehrzeilendarstellung der hosts **gwdl001**, **gwdl002** und **gwdl003**

   bhosts -l gwdl001 gwdl002 gwdl003

4.4 Fehlerquellen

„command not found“ oder Ähnliches bei Verwendung von LSF-Kommandos

Die zu LSF gehörigen Umgebungsvariablen wurden nicht richtig gesetzt. Sie können dies in der Kommandozeile tun. Für ksh und bash lautet der Befehl

```
. /opt/hplsf/conf/profile.lsf
```

Für csh und tcsh:

```
source /opt/hplsf/conf/cshrc.lsf
```

Fehlende Bibliotheken bei Submittierung zwischen verschiedenen Architekturen

Wenn von einer Architektur auf eine andere submittiert wird - z. B. von der **gwdu102** (Linux) in die **gwdg-rs6k-**queue (AIX) - kann es zu Fehlermeldungen bezüglich fehlender Bibliotheken kommen. Bitte submittieren Sie in diesem Fall von derselben Architektur, die auch Ziel für die Ausführung des Jobs ist, und teilen Sie uns das Problem mit.

Programm „hängt“ bei Verwendung einer STDIN-pipe

Wenn mittels des **<**-Zeichens z. B. eine Datei **inputfile** in den STDIN-Strom eines Programms eingelesen wird, bleibt dieses stehen. Dieses Problem tritt bei Submittierung mit der **-a openmp** Option auf. Verwenden Sie in dem Fall **cat** zum Bilden der pipe, also

```
bsub -a openmp ... 'cat inputfile |
smpprog'
```

statt wie bisher

```
bsub -a openmp ... smpprog < inputfile
```

Dies gilt analog auch für Skripten.

Boehme

---

5. IT-Sicherheitsleitlinie der GWDG

5.1 Vorbemerkung

Sicherheit der IT-Infrastruktur bedeutet kurz gefasst Gewährleistung von Vertraulichkeit, Verfügbarkeit und Integrität von IT-Systemen. Der Weg zur Herstellung und Erhaltung von IT-Sicherheit ist der IT-Sicherheitsprozess, den das BSI in seinem Grundschutzhandbuch wie folgt beschreibt:

- Initiierung des IT-Sicherheitsprozesses

  Erstellung einer IT-Sicherheitsleitlinie

  Einrichtung eines IT-Sicherheitsmanagements

- Erstellung eines IT-Sicherheitskonzepts

  IT-Strukturanalyse

  Schutzbedarfsfeststellung

  IT-Grundschutzanalyse

  ggf. ergänzende Sicherheitsanalyse

  Realisierungsplanung

- Umsetzung

- Aufrechterhaltung im laufenden Betrieb

Man erkennt leicht, dass der erste Schritt des Sicherheitsprozesses die Erstellung einer IT-Sicherheitsleitlinie ist. In diesem Artikel soll über die IT-Sicherheitsleitlinie der GWDG selbst und ihre Erstellung und Einführung bei der GWDG sowie über die Dienste, die die GWDG den Einrichtungen der Max-Planck-Gesellschaft und der Universität Göttingen in diesem Umfeld anbietet, berichtet werden.

5.2 Erstellungs- und Einführungsprozess

Die Erstellung und Einführung einer Sicherheitsleitlinie ist kein Unterfangen, das in wenigen Tagen erledigt werden kann. Da es ja ein Dokument mit langer Lebensdauer sein soll, wird man Inhalte und Formulierungen gründlich durchdenken müssen. Zudem sind viele Abstimmungen nötig, bevor mit der Einführung begonnen werden kann.

Von ersten Vorüberlegungen Anfang 2002 bis zu einem ersten Entwurf hat die GWDG ca. vier Monate benötigt. Die Überarbeitung bis zu einer Festlegung der Formulierung hat wiederum einen Monat gekostet. Abstimmungsprozesse im Beirat und Aufsichtsrat der GWDG sowie mit dem eigenen Betriebsrat haben dann wiederum mehrere Monate gedauert, bis auch eine von diesen Gremien akzeptierte Version erstellt war.

Diese Leitlinie wurde dann innerhalb der GWDG zum 01.06.2003 probeweise eingeführt. Die Einschränkung „probeweise“ wurde gemacht, um den Mitarbeitern zu signalisieren, dass hier auch geprüft werden sollte, inwieweit die in der Leitlinie festgeschriebenen Maßnahmen und Strukturen sich in der Praxis bewähren.

Als Ergebnis der Probephase wurden kleinere Änderungen vorgenommen. Seit dem 01.03.2004 hat die GWDG eine uneingeschränkt gültige IT-Sicherheitsleitlinie.

5.3 Inhalt der Leitlinie der GWDG

Eine IT-Sicherheitsleitlinie legt keine Detailregelungen fest. Sie beschreibt vielmehr allgemeine Ziele, Strategien und Organisationsstrukturen. Diese spiegelt sich in der Gliederung der Leitlinie der GWDG wieder:

1. Sicherheitsziele und Sicherheitsstrategie
2. Umsetzung
3. Organisation
4. Verantwortlichkeiten
5. Durchsetzung
6. Übergangsregelungen
7. Inkrafttreten

Sicherheitsziele und Sicherheitsstrategie

In diesem Kapitel finden sich Unterpunkte zum Stellenwert der IT-Sicherheit, zum Sicherheitsbewusstsein, zu Sicherheitszielen und zur Sicherheitsstrategie.

Der Abschnitt **„Stellenwert der IT-Sicherheit“** stellt die Bedeutung der IT-Sicherheit für die GWDG nach innen und außen dar.

Der Abschnitt **„Sicherheitsbewusstsein“** richtet sich primär an die Beschäftigten der GWDG. Er lautet:

„Die Informationssicherheit ist ein zunehmend wichtiger Faktor geworden. Daraus folgt, dass das Sicherheitsbewusstsein einer der entscheidenden Erfolgsfaktoren für die GWDG ist.

Sicherheitsbewusstsein ist durch folgendes Verhalten gekennzeichnet:

- *Erkennen, dass effektive Sicherheit eine kritische und wesentliche Geschäftsgrundlage ist.*
- *Stets vorhandenes Sicherheitsbewusstsein bei allen täglich anfallenden Aktivitäten.*
- *Persönliche Verantwortlichkeit für präventive Maßnahmen in Bezug auf sämtliche Risiken für Mitarbeiter, Informationen, IT-Systeme, Vermögenswerte und die Fortführung der Geschäftstätigkeit im Notfall.“*

Unter **„Sicherheitsziele“** werden allgemeine Ziele aufgeführt:

„Das gesamte IT-System muss so geschützt werden, dass

- *die Vertraulichkeit in angemessener Weise gewahrt ist,*
- *die Integrität des gesamten IT-Systems sichergestellt ist,*
- *es bei Bedarf verfügbar ist,*
- *die Beteiligung an einem sicherheitsrelevanten IT-Vorgang nicht geleugnet werden kann (Verbindlichkeit),*
- *es gesetzliche, vertragliche und aufsichtsrechtliche Verpflichtungen erfüllen kann.*

Es wird verlangt, dass

- *der jeweils für die IT-Systeme geltende Sicherheits- und Kontrollumfang am jeweiligen Betriebsrisiko ausgerichtet ist,*
- *für alle Teile des gesamten IT-Systems (Rechner, Daten und Verfahren) namentlich Systemverantwortliche ernannt werden,*
- *die einzelnen Nutzer für die sachgerechte Nutzung des IT-Systems verantwortlich sind,*
- *durch Erzeugung zusätzlicher Informationen und durch zusätzliche Verfahren die Nachvollziehbarkeit sämtlicher sicherheitsrelevanter IT-Vorgänge gewährleistet ist,*
- *es eine Überprüfung der Verwaltung und Nutzung von IT-Systemen gibt.“*

Wesentlich konkreter wird die Leitlinie im Abschnitt **„Sicherheitsstrategie“**.

„Die Sicherheitsstrategie basiert auf folgenden Prinzipien:

- *Schulung der Mitarbeiter und Nutzer*
- *Betrieb von Server-Systemen nur in grundsätzlich verschlossenen und zugangsüberwachten Räumen,*

- *personenbezogene Authentifizierung für Systemzugriffe (außer für ausdrücklich anonyme Dienste wie WWW-Seiten usw.),*
- *Einführung sicherer Authentifizierungsverfahren,*
- *Beschränkung von Zugriffsrechten auf die für die Aufgabenerfüllung notwendigen Rechte,*
- *sichere Konfiguration der IT-Systeme durch Beschränkung der installierten Software und aktivierten Dienste auf die für die Funktion der Systeme benötigten Komponenten,*
- *sichere Konfiguration der IT-Systeme durch zeitnahe Implementation aller veröffentlichter sicherheitsrelevanter Software-Korrekturen,*
- *Strukturierung des Netzes entsprechend der benötigen Sicherheitsniveaus und Unterbindung aller nicht notwendigen Zugriffsmöglichkeiten auf IT-Systeme,*
- *Verzicht auf Systeme, die eine Übertragung unverschlüsselter Passwörter oder passwortähnlicher Informationen verlangen,*
- *Einsatz verschlüsselter Übertragungsverfahren soweit technisch realisierbar und soweit eine Vertraulichkeit der Inhalte gegeben ist,*
- *verschlüsselte Speicherung sensibler Daten,*
- *Datenhaltung ausschließlich auf dedizierten Daten-Servern und tägliche Sicherung ihrer Daten,*
- *räumliche Trennung von Daten-Servern und Backup-Systemen.“*

Umsetzung

Die wesentlichen Teile der Kapitels Umsetzung sind Organisation, Konzeption, Sicherheitsdokumentation sowie Schulung und Einweisung.

„Organisation“ beschreibt die im Sicherheitsprozess beteiligten Gruppierungen.

„Die IT-Sicherheit der GWDG wird als zentrale Aufgabe betrachtet. Die Bewältigung dieser Aufgabe erfolgt durch das Sicherheitsmanagement der GWDG, das durch

- *den IT-Sicherheitsbeauftragten und*
- *das IT-Sicherheitsmanagement-Team*

gebildet wird, im Zusammenspiel mit anderen Organisationseinheiten, namentlich

- *Geschäftsführung der GWDG,*
- *Gruppenleitern der GWDG,*
- *Systembetreuern,*
- *Nutzern und*
- *externen Dienstleistern.*

Die Aufgabenverteilung auf diese Rollen ist im Abschnitt „Verantwortlichkeiten“ beschrieben.“

„Konzeption“ beschreibt das Grundkonzept zur Umsetzung der Sicherheitsziele:

„Die Umsetzung der Sicherheitsziele entsprechend der Sicherheitsstrategie erfolgt durch das Sicherheitskonzept der GWDG bestehend aus

- *dieser **IT-Sicherheitsleitlinie**, die Sicherheitsziel, Sicherheitsstrategien und die Konzeption definiert,*
- ***allgemeinen Sicherheitsstandards** für verschiedene Typen von IT-Systemen und*
- ***systemspezifischen Sicherheitsrichtlinien** für einzelne IT-Systeme oder Gruppen von IT-Systemen.*

Als allgemeiner Sicherheitsstandard gilt dabei die aktuelle Version des Grundschutzhandbuchs des Bundesamts für Sicherheit in der Informationstechnik (BSI), ggf. ergänzt oder modifiziert durch eigene Sicherheitsstandards der GWDG.

Alle IT-Systeme einschließlich ihres Einsatzzwecks sind zu erfassen und bezüglich des Sicherheitsrisikos und ihres Schutzbedarfs zu analysieren und zu klassifizieren. Auf der Basis dieser Sicherheitsklassifizierung sowie der IT-Sicherheitsleitlinie und den allgemeinen Sicherheitsstandards sind für jedes IT-System bzw. für Gruppen gleichartiger IT-Systeme die systemspezifischen Sicherheitsrichtlinien festzulegen.

Für jedes IT-System ist für Betrieb und Sicherheit ein Systemverantwortlicher namentlich zu benennen.

Prinzipiell ist der für ein Gerät (Rechner, Infrastrukturkomponente und sonstige Hardware) benannte Systemverantwortliche für alle auf dem Gerät systemseitig von der GWDG bereitgestellte Software und Informationen sowie für damit bewältigten Prozesse verantwortlich, solange kein Systemverantwortlicher für diese Teil-IT-Systeme benannt wird.

Die Sicherheitsrisikoanalyse ist ein fester Bestandteil bei der Entwicklung, bei Einführungs- und Wartungsverfahren von IT-Systemen, und zwar ab Beginn und während des gesamten Lebenszyklus.

Neue IT-Systeme müssen dem Sicherheitskonzept entsprechen und dürfen erst nach erfolgter Sicherheitsklassifizierung und Festlegung systemspezifischer Sicherheitsrichtlinien in Produktion genommen werden.“

Die weiteren Abschnitte dieses Kapitels beschreiben im Wesentlichen die Dokumentation des Sicherheitsprozesses und Schulungsmaßnahmen.

Verantwortlichkeiten

In diesem Kapitel wird festgelegt, wie Verantwortlichkeiten auf die unter „Organisation“ aufgeführten Beteiligten verteilt werden. Die Regelungen sollen hier nicht im Detail aufgeführt werden. Grundprinzipien sind:

- Die Gesamtverantwortung für die Sicherheit des gesamten IT-Systems hat die Geschäftsführung.
- Verantwortlichkeiten für IT-Sicherheit werden innerhalb der Organisationsstruktur der GWDG genauso delegiert wie die Verantwortlichkeiten für alle anderen Aufgaben. Insbesondere liegt die Verantwortung für den Betrieb aller IT-Systeme einer Arbeitsgruppe beim zuständigen Gruppenleiter.
- Verantwortlichkeiten für Detailplanungen und Umsetzungen werden dann zu den Systemverantwortlichen delegiert.

Die Funktion des Sicherheitsmanagements (IT-Sicherheitsbeauftragter plus IT-Sicherheitsmanagement-Team) sind wie folgt definiert:

„Das Sicherheitsmanagement ist verantwortlich für

- *die Erstellung, Überprüfung, Entwicklung, Fortschreibung und Veröffentlichung der IT-Sicherheitsleitlinie,*
- *die Erstellung, Überprüfung, Entwicklung, Fortschreibung und Veröffentlichung der allgemeinen Sicherheitsstandards,*
- *die Überprüfung der Stichhaltigkeit der Klassifizierung von IT-Systemen entsprechend des Sicherheitsrisikos und Schutzbedarfs,*
- *die Stellungnahmen zu den von den Systemverantwortlichen erstellten systemspezifischen Sicherheitsrichtlinien,*
- *Veranlassung und/oder Durchführung von Einweisungen und Schulungen in die IT-Sicherheit,*
- *die Erstellung von Berichten zur IT-Sicherheit an die Geschäftsführung.*

Das Sicherheitsmanagement ist bezüglich der Festlegung von Einsatzzwecken von IT-Systemen und der systemspezifischen Sicherheitsrichtlinien zu informieren. Kommt das Sicherheitsmanagement zu dem Schluss, dass Klassifizierungen von IT-Systemen, Einsatzzwecke oder systemspezifische Sicherheitsrichtlinien mit der Sicherheitsleitlinie und/oder den allgemeinen Sicherheitsstandards nicht konform sind oder erhebliche Risiken bedingen, so hat das Sicherheitsmanagement diese Bedenken den zuständigen Systemverantwortlichen und Gruppenleitern vorzutragen und ggf. der Geschäftsführung zwecks Entscheidung vorzulegen.

Das Sicherheitsmanagement versichert sich regelmäßig der Einhaltung dieser Leitlinie und veranlasst regelmäßige Überprüfungen bezüglich der Einhaltung der Sicherheitsstandards und Sicherheitsrichtlinien durch den Systemverantwortlichen oder durch Dritte in Absprache mit dem Systemverantwortlichen oder führt diese Überprüfung in Absprache mit dem Systemverantwortlichen selbst durch.

Das Sicherheitsmanagement ist für die Eskalation festgestellter und nach dem Sicherheitskonzept nicht vorgesehener Risikoübernahmen an die Geschäftsführung verantwortlich.“

Durchsetzung, Übergangsregelungen und Inkrafttreten

Unter **„Durchsetzung“** wird ausdrücklich bewusst gemacht, dass Verstöße gegen die IT-Sicherheitsleitlinie entsprechend der gesetzlichen Bestimmung sanktioniert werden können.

„Übergangsregelungen“ sind trotz der oben beschrieben langen Vorlaufzeit dennoch vorgesehen, denn ein vollständige Umsetzung des Gesamtkonzepts war vor Inkrafttreten der Regelung noch nicht in allen Details möglich.

5.4 IT-Sicherheitsleitlinien für Max-Planck-Institute und die Universität Göttingen

Nun sollte sicherlich nicht nur die GWDG in ihrem eigenen Bereich IT-Sicherheit realisieren. Auch Max-Planck-Institute und die Universität Göttingen haben diesen Bedarf erkannt. Folgt man den Vorschlägen des BSI, so sollte auch hier mit der Initiierung eines Sicherheitsprozesses begonnen werden, in dem eine Sicherheitsleitlinie erstellt wird.

Diese Einrichtungen haben eine von der GWDG deutlich abweichende Größe und Struktur, so dass die Leitlinie der GWDG sicherlich nicht direkt übernommen werden kann. Dennoch können die Grundkonzepte dieser Leitlinie einen Startpunkt für andere geben.

Für die Max-Planck-Gesellschaft hat die GWDG bereits im September 2002 dem BAR der MPG ein aus dem damaligen Entwurf der GWDG-Leitlinie abgeleitetes Grundkonzept einer Leitlinie für ein Max-Planck-Institut vorgelegt.

Von der Universität Göttingen hat die GWDG den Auftrag erhalten, einen Entwurf für eine IT-Sicherheitsleitlinie der Universität zu erstellen. Hier werden noch mehr Abweichungen – insbesondere im organisatorischen Bereich – gegenüber der GWDG-Leitlinie nötig sein, als in dem Entwurf für die MPG.

Beck

6. Der Videokonferenzdienst des DFN-Vereins und seine Nutzung über den Gatekeeper der GWDG

6.1 Einleitung

Der folgende Artikel enthält im ersten Teil eine Beschreibung des Videokonferenzdienstes des DFN-Vereins und im zweiten Teil Hinweise auf die Nutzungsmöglichkeit des Videokonferenzdienstes über den Gatekeeper der GWDG. Der erste Teil gibt im Wesentlichen die Beschreibung des DFNVC-Dienstes auf den WWW-Seiten des Videokonferenzportals wieder.

6.2 DFNVC – der Videokonferenzdienst im deutschen Wissenschaftsnetz

6.2.1 Überblick über den Dienst DFNVC (DFN-VideoConference)

Der DFN-Verein bietet den Wissenschaftlern in Deutschland die Möglichkeit, über den *Videokonferenzdienst DFNVC* und das Gigabit-Wissenschaftsnetz (G-WiN) multimedial mit Kollegen an anderen Hochschulen und Forschungseinrichtungen zu kommunizieren. DFNVC ist speziell auf die Anforderungen wissenschaftlicher Nutzer zugeschnitten und kann direkt vom Arbeitsplatz aus über PCs und Laptops sowie Videokonferenz-Raumsysteme oder Telefone genutzt werden. Der Dienst ermöglicht Videokonferenzen mit einer Vielzahl von Teilnehmern und steht den Nutzern rund um die Uhr ohne vorherige Planung und Reservierung zur Verfügung. Zusätzlich zur Videokonferenz besteht die Möglichkeit, Daten wie beispielsweise Arbeitsdokumente auszutauschen. Folgende Aspekte machen den Dienst interessant:

- Durchführung von Mehrpunktkonferenzen direkt vom Arbeitsplatz oder vom Raumsystem in der Arbeitsumgebung unter Nutzung der DFN-Multipoint-Control-Unit (MCU), einer technischen Komponente zum Sammeln und Verteilen multimedialer Datenströme
- Internationale Erreichbarkeit über die Gatekeeper-Struktur mit einem abgestimmten Nummernplan zur Adressierung der Kommunikationspartner
- Einbinden von ISDN-Teilnehmern in die Konferenz über einen Gateway
- Audiokonferenzen vom PC-Arbeitsplatz oder vom ISDN-Telefon ohne zusätzliche Beschaffungen
- Auswählen von speziellen Videoübertragungsparametern und Videodarstellungen sowie Einbeziehung von verteilten Anwendungen in Konferenzen über das Protokoll T.120 (z. B. Übertragen von Folien oder Arbeiten an einer gemeinsamen Applikation)
- Effektive Nutzung der Netzressourcen
- Unterstützung der Administration durch DFN-Hotline und Schulung
- Verständliche Benutzeroberfläche auch für Nichtfachleute

Eine kleine Auswahl an Anwendungsbeispielen soll die Vielzahl der Einsatzmöglichkeiten von Videokonferenzsystemen verdeutlichen:

Konferenzen von Rektoren, Präsidenten, Kanzlern und Leitern von Rechenzentren und anderen Einrichtungen

Direktoren oder Rechenzentrumsleiter können schnell und flexibel Entscheidungen treffen, wenn sie ihre Besprechungen über eine Videokonferenz durchführen.

Übertragungen von Vorlesungen

Studenten können Vorlesungen von zu Hause aus verfolgen oder an einem Seminar aktiv teilnehmen.

Austausch von Unterlagen / gemeinsames Bearbeiten

Institute mit verschiedenen Standorten sind an Außenmessungen beteiligt; die Ergebnisse liegen nur an einem Standort vor. Während einer Videokonferenz werden diese Ergebnisse über ein Desktop oder Whiteboard angezeigt und bearbeitet.

Gemischte Video- und Telefonkonferenzen

In einer Videokonferenz werden Forschungsergebnisse diskutiert. Ein Experte, der nicht über ein Videokonferenzsystem verfügt, oder ein Teilnehmer auf Reisen kann über das Telefon hinzugezogen werden.

Abwicklung von Auswahlgesprächen und Tests

Für ein erstes Vorstellungsgespräch können Bewerber ohne Reiseaufwand über eine Videokonferenz eingeladen und begutachtet werden. Auf diesem Wege können auch Tests und Prüfungen durchgeführt werden.

6.2.2 Technik des Dienstes DFNVC

Der Dienst DFNVC überträgt die audiovisuellen Datenströme über das Wissenschaftsnetz und nutzt dafür das international standardisierte Protokoll H.323, das die Datenübertragungen für Audio-, Video- und Datenkonferenzen regelt. Den Nutzern eröffnen sich dadurch neue Dimensionen des Arbei-

tens im Netz. Durch direkte Verbindungen zwischen dem Wissenschaftsnetz und den Forschungsnetzen in Europa, Nordamerika und weltweit sowie mit Hilfe eines international abgestimmten Nummernplans zum Adressieren der Konferenzpartner - dem *Global Dialing Scheme* ***GDS*** - ermöglicht der Dienst DFNVC außerdem den Aufbau internationaler Videokonferenzen.

Dank der hohen Übertragungsleistungen und der breitbandigen Verbindungen des Wissenschaftsnetzes bietet der Dienst auch bei Konferenzen mit mehreren Teilnehmern eine gute Ton- und Bildqualität.

Kernstück des Dienstes DFNVC sind die so genannten Multipoint Control Units (MCUs), die Mehrpunktkonferenzen ermöglichen und die Organisation der multimedialen Datenströme übernehmen.

In einem so genannten Zonen-Konzept werden alle Videokonferenzgeräte auf verteilten Gatekeepern registriert. Diese übernehmen die Rufweiterleitung und die Adressierung der Konferenzpartner. Basis für die Übertragung der Video- und Audio-Daten sind der Dienst *DFNInternet* und die Videokonferenzinfrastruktur des DFN-Vereins, über die Video- und Audio-Konferenzen entsprechend der Verfügbarkeit der hierfür notwendigen technischen Komponenten durchgeführt werden können. Die für den Dienst DFNVC realisierte Struktur ist in Abbildung 1 dargestellt.

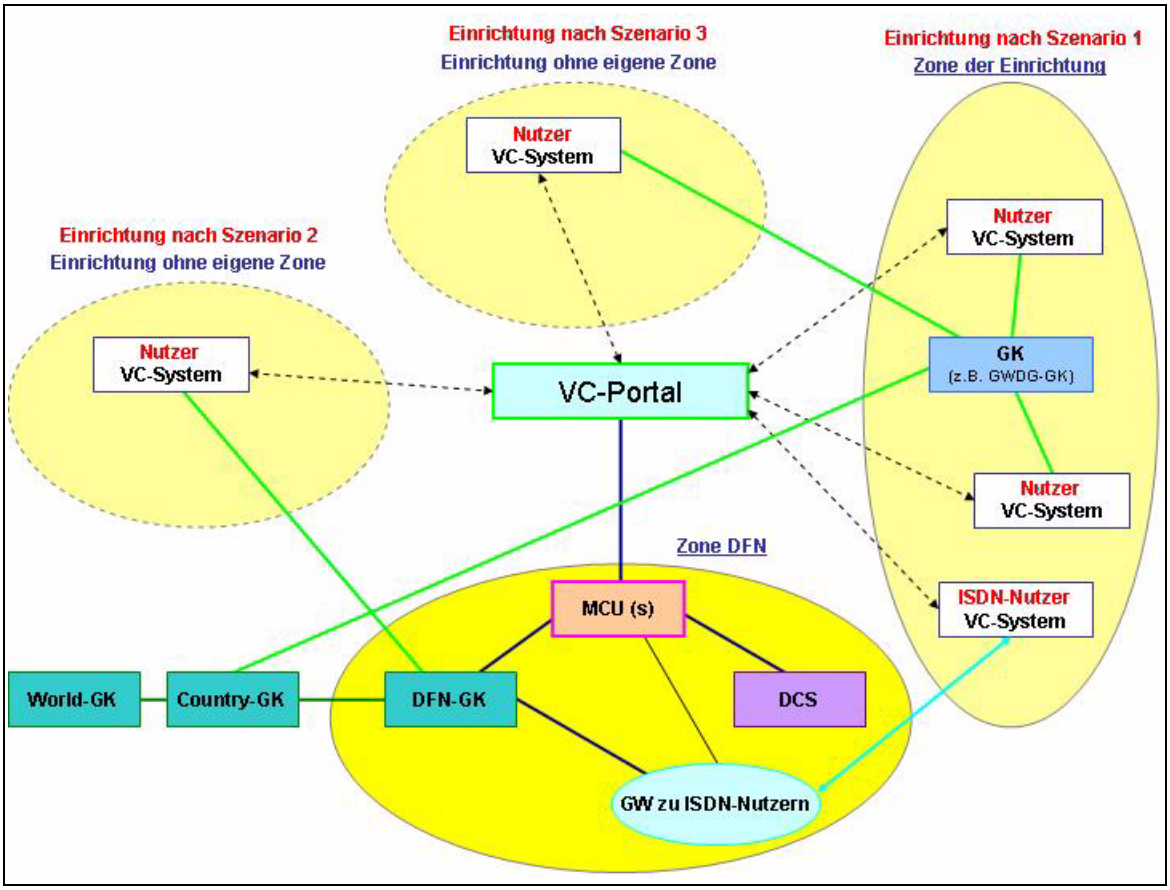

Abb. 1: Architektur des Dienstes DFNVC

(Quelle: den Web-Seiten des DFN-Vereins mit freundlicher Genehmigung entnommen)

Legende:

Einrichtung:	eine Hochschule oder Forschungseinrichtung, die einen Vertrag zur Nutzung des Wissenschaftsnetzes abgeschlossen hat
Nutzer:	Studierender, Mitarbeiter oder Gast einer Einrichtung
VC-System:	Videokonferenzendsystem

Legende:

GK:	Gatekeeper: Hard- oder Software-Komponente mit Funktionalitäten u. a. zur Rufweiterleitung und Adressierung der Videokonferenzendsysteme der Konferenzpartner
Country GK:	Gatekeeper unter der Adressierungsnummer 0049, über den die nationalen (Country GK) und internationalen Partner (World GK) erreichbar sind
MCU:	Multipoint Control Unit: Sternverteiler für Gruppenkonferenzen. Eine MCU ist eine Hard- und/oder Software-Lösung, die eine oder mehrere Mehrpunktkonferenzen verwaltet.
DCS:	Data Collaboration System zur Durchführung von Datenanwendungen wie z. B. Application Sharing oder Chat, basierend auf dem Protokoll T.120
GW:	Gateway zwischen den Protokollwelten H.323 (IP) und H.320 (ISDN); ermöglicht die Teilnahme von ISDN-Systemen in einer Konferenz
Zone:	Nach H.323 ist eine Zone ein Bereich, der H.323-Komponenten wie MCUs, Gateways und VC-Systeme enthält, die genau von einem Gatekeeper verwaltet werden.
VC-Portal:	Das VC-Portal ist eine web-basierte Sammlung von Informationen und Dokumentationen zum Dienst DFNVC sowie die Schnittstelle zur Nutzerunterstützung für Konferenzvorbereitung und -aufbau (**`http://www.vc.dfn.de`**).

6.2.3 Nutzungsarten des DFNVC

Möchte eine Einrichtung den DFNVC-Dienst nutzen, so hat sie die Wahl zwischen drei Szenarien, die sich in der Art und Weise der Registrierung der Videokonferenzsysteme auf einem Gatekeeper sowie in der Unterstützung der Nutzer unterscheiden. Folgende Nutzungsarten sind möglich:

Szenario 1: Nutzung mit eigener H.323-Zone der Einrichtung

Die Einrichtung betreibt für sich (ggf. auch für eine oder mehrere andere Einrichtungen) eine H.323-Zone mit dem dafür notwendigen Gatekeeper. Der Administrator dieser Einrichtung ist für alle technischen und organisatorischen Belange seiner Nutzer (und ggf. auch der Nutzer anderer Einrichtungen) zuständig. Er kann die Hotline des DFNVC-Dienstes in Anspruch nehmen.

Szenario 2: Direkte Nutzung über die DFN-Zone

Die Nutzer einer Einrichtung, die keine eigene H.323-Zone mit zugehörigem Gatekeeper betreibt, können den Dienst DFNVC über die DFN-Zone und den DFN-Gatekeeper nutzen. Diese Nutzungsart wird in der Regel nur von Einrichtungen mit geringem Konferenzbedarf und wenigen Videokonferenzendgeräten beauftragt. Der Nutzer wendet sich in allen technischen Fragen direkt an die DFNVC-Hotline.

Szenario 3: Nutzung über die H.323-Zone einer anderen Einrichtung

Die Nutzer dieser Einrichtung nutzen den Dienst über die H.323-Zone und den Gatekeeper einer anderen Einrichtung. Für alle technischen und organisatorischen Belange der Nutzer ist der Administrator der anderen Einrichtung zuständig.

6.2.4 Die Suche nach einem geeigneten Videokonferenzsystem

Ein Nutzer, der erstmalig eine Videokonferenz durchführen möchte, muss sich zunächst um ein geeignetes Videokonferenzsystem kümmern. Je nach Anwendungsumgebung kommen verschiedene Systeme zum Einsatz.

Will man Videokonferenzen von seinem gewohnten Arbeitsplatz aus durchführen, so muss der PC oder Laptop mit einem so genannten Desktop-System aufgerüstet werden (ab ca. 180,- Euro pro Arbeitsplatz inkl. Kamera und Headset als Software-Lösung, ab ca. 350,- Euro als Hardware-Lösung). Die Systeme werden über eine USB-Schnittstelle oder Steckkarte angeschlossen und bieten volle interaktive Audio-/Video-Funktionalität. Beispiele hierfür sind die Systeme Polycom ViaVideo, VCON Vigo und die Software-Clients eConf und Microsoft Netmeeting.

Soll ein Seminar- oder Schulungsraum ausgestattet werden, so bieten sich so genannte Settop-Systeme mit einem Monitor an, mit denen z. B. Treffen von Arbeitsgruppen möglich werden (ab ca. 6.000,- Euro erhältlich). Diese kompakten Settop-Einheiten wie z. B. die Systeme Polycom Viewstation, Sony Contact 1600, Tandberg 880 und VCON Falcon IP sind passend für jeden Standard-TV-Monitor und werden meist auf dem Monitor platziert.

Etwas teurer und aufwändiger wird es bei der Ausstattung von großen Konferenzräumen mit so genannten Raumsystemen, die über 1-2 Monitore,

Rollwagen und Übertragungsbandbreiten bis zu 2 Mbps über ISDN und 3 Mbps über IP verfügen.

Bei Auswahl und Einsatz von Videokonferenzsystemen bietet das vom DFN-Verein betriebene Kompetenzzentrum für Videokonferenzdienste (VCC) an der TU Dresden wertvolle Hilfe an. Im WWW ist das VCC unter dem URL

http://vcc.urz.tu-dresden.de

zu finden. Das VCC untersucht laufend aktuelle Videokonferenz-Hardware und -Software. Für die bekanntesten Systeme wurden ausführliche Tests durchgeführt und die Ergebnisse dokumentiert. Im WWW finden sich zahlreiche Produktinformationen über die gängigen Desktop-, Kompakt- und Raumsysteme sowie Installationsanleitungen. Das VCC unterstützt die DFN-Einrichtungen bei der Einsatzplanung, der Installation und dem Betrieb von Videokonferenzkomponenten. Eine Beratung und Betreuung der Einrichtungen wird über Telefon oder über E-Mail geleistet. Zur Lösung von Problemen können auch Testkonferenzen aufgesetzt werden. Zusätzliche Informationen können in den regelmäßig stattfindenden Workshops gewonnen werden. Darüber hinaus findet eine konkrete Beratung zur Verwendung von geeignetem Audio- und Video-Equipment (Mikrofone, Kameras etc.) statt. Bei Auswahl und Einsatz eines Gatekeepers kann ebenfalls auf umfassende Beratung sowie auf Installationshilfen zurückgegriffen werden.

Für Einrichtungen, die am Dienst DFNVideoConference teilnehmen wollen, werden vorab Schulungen durchgeführt, wodurch die lokalen Administratoren eine praktische Einführung in ihre zukünftigen Arbeiten bekommen. Als Einarbeitung in die Thematik Videoconferencing stellt der DFN-Verein unter

http://vcc.urz.tu-dresden.de/vc-handbuch/

ein kostenloses Videokonferenzhandbuch bereit.

6.2.5 Das VC-Portal des DFNVC - zentraler Einstiegspunkt ins DFNVC

Zentraler Einstiegspunkt von DFNVC ist ein vom DFN-Verein bereitgestelltes Portal, das unter der Adresse

https://www.vc.dfn.de

erreichbar ist. Hier werden alle dienstrelevanten Informationen angeboten. Neben dem internationalen Nummernplan für Gatekeeper und Endsysteme finden sich auf dem Portal die Dienst- und Leistungsbeschreibungen, Schulungsunterlagen, Dokumentationen und aktuelle Mitteilungen für die Nutzer. Darüber hinaus bietet das VC-Portal Unterstützung beim Konferenzaufbau, beim Steuern von Konferenzen sowie einen Passwort-Schutz für Konferenzen. In einem Verzeichnis werden alle angemeldeten bzw. aktiven Endsysteme in der DFN-Zone und auch in den Zonen externer Einrichtungen angezeigt, was eine einfache Organisation spontaner Videokonferenzen ermöglicht. Wichtige Konferenzen können auf Wunsch von einem Operateur des DFN-Vereins betreut werden. Eine speziell eingerichtete DFN-Hotline unterstützt Videokonferenzadministratoren in den Rechenzentren der Hochschulen und je nach gewählter Nutzungsart auch die Nutzer in den Einrichtungen bei der Einführung und beim Betrieb des Dienstes.

6.2.6 Weitere Informationen

Weitere Informationen sind unter folgenden Adressen erhältlich:

- auf der DFN-Seite **http://www.dfn.de** unter Dienstleistungen -> DFNVC
- auf dem VC-Portal **https://www.vc.dfn.de**
- bei der Hotline unter **hotline@vc.dfn.de**.

Umfangreiche Informationsmaterialien zum Dienstleistungsangebot DFNVideoConference können als PDF-Dateien unter folgenden Adressen von den WWW-Seiten des DFN-Vereins bezogen werden:

- DFNVC-Flyer

  http://www.dfn.de/uploaded/DFNVC-Flyer.pdf

- DFNVC - Einstieg in die Technik

  http://www.dfn.de/uploaded/DFNVC-Technik-Info.pdf

- Leistungsbeschreibung DFNVC

  http://www.dfn.de/uploaded/dfnvc_lb.pdf

6.3 Videokonferenzen über den Gatekeeper der GWDG

6.3.1 Warum eine Anbindung an den GWDG-Gatekeeper?

Die GWDG hat mit dem DFN-Verein einen Vertrag zur Nutzung des Videokonferenzdienstes *Szenario 1: Nutzung mit eigener H.323-Zone der Einrichtung* und kann diesen Dienst somit der Universität Göttingen und der Max-Planck-Gesellschaft sowie den weiteren nutzungsberechtigten wissenschaftlichen Einrichtungen anbieten.

Wie bereits in den GWDG-Nachrichten 8/2003 im Artikel „Videokonferenzen mit dem Gatekeeper der GWDG“ beschrieben, betreibt die GWDG einen GNU-Gatekeeper mit Proxy-Funktionalität. Durch die Registrierung an diesen Gatekeeper steht den Benutzern der Videokonferenzdienst des DFN-Vereins zur Verfügung. Er beinhaltet die Nutzung der

DFN-MCU für Mehrpunkt-Konferenzen und die Nutzung des ISDN-Gateways zur Verbindungsaufnahme von Videokonferenzsystemen zwischen TCP/IP-Netzen und der ISDN-Welt. Der GWDG-Gatekeeper ist neben anderen Gatekeepern an den Country-Gatekeeper des DFN-Vereins angebunden. Dieser ist wiederum in einem weltweiten Gatekeeper-Verbund vernetzt. So können über dieses Netzwerk Videokonferenzen weltweit durchgeführt werden. Die Proxy-Funktionalität des GWDG-Gatekeepers ermöglicht zusätzlich die Durchführung von Videokonferenzen zwischen Videokonferenzendgeräten im geschützten TCP/IP-Netz der GWDG und dem weltweiten Internet.

6.3.2 Anmeldung von Videokonferenzendgeräten am GWDG-Gatekeeper

Benutzer, die den Videokonferenzdienst des DFN-Vereins nutzen möchten, sollten sich unter Verwendung des E.164-Nummern-Schemas am GWDG-Gatekeeper registrieren. Für die Anmeldung am GWDG-Gatekeeper müssen in den Videokonferenzendgeräten folgende Eintragungen durchgeführt werden:

1. die IP-Adresse des GWDG-Gatekeepers und
2. eine E.164-Nummer und ein Alias-Name für das jeweilige Videokonferenzendgerät.

Damit eine eindeutige strukturierte Zuordnung gewährleistet wird, werden die E.164-Nummern und die Alias-Namen für die Videokonferenzendgeräte in Absprache mit der GWDG vergeben. Zur Registrierung am GWDG-Gatekeeper und zur Beratung bei der Nutzung des Videokonferenzdienstes des DFN-Vereins ist Ihnen Herr Thomas Körmer (E-Mail: tkoerme@gwdg.de) gern behilflich.

Eine Anleitung zur Anbindung bzw. Konfiguration von Videokonferenzsystemen verschiedener Hersteller an einen Gatekeeper ist unter der Adresse

`http://vcc.urz.tu-dresden.de/vc-systeme/konfiguration/`

des Kompetenzzentrums für Videokonferenzdienste an der TU Dresden verfügbar.

6.3.3 E.164-Nummern-Schema und Arbeitsweise des GWDG-Gatekeeper

Der Gatekeeper der GWDG ist eine logische Komponente des H.323-Standards, der die Videokonferenzdienste über das Internet-Protokoll definiert. Alle Videokonferenzendgeräte, die an ihm registriert sind, befinden sich in einer gemeinsamen H.323-Zone. In Absprache mit dem DFN-Verein erhalten innerhalb dieser Zone alle Endgeräte zur eindeutigen Kennzeichnung eine E.164-Nummer nach einem international festgelegten E.164-Nummern-Schema. An zwei Beispielen soll dieses Schema für Videokonferenzendgeräte in der GWDG-Zone erläutert werden:

00495513904467 und 004955120101552

0049	Landeswahl „Deutschland“
551	GWDG-Gatekeeper-Zone (551 ist die Vorwahl von Göttingen)
39 bzw. 201	aus dem Hauptanschluss genommene Zahlen (hier Universität Göttingen bzw. MPI für biophysikalische Chemie / GWDG)
0	Zusatz zur Kennzeichnung der Nummer als eine E.164-Nummer
4467 bzw. 1552	die Nebenanschluss-Nummer eines Telefons im Videokonferenzraum

Weiterhin sollte jedes Videokonferenzsystem zur besseren Identifizierung einen Alias-Namen erhalten, der in der GWDG-Zone nach folgendem Muster gebildet wird.:

[Ort] - [Institutskürzel] - [Name/Standort]

Zwei Beispiele für einen Alias-Namen sind:

goe-gwdg-maier und goe-uzpr-konferenzraum

Sind die Videokonferenzendgeräte am GWDG-Gatekeeper angemeldet, werden im Gatekeeper die E.164-Nummern den entsprechenden dazugehörigen IP-Adressen zugeordnet. Die Videokonferenzsysteme können nun durch den Ruf der E.164-Nummern miteinander Verbindung aufnehmen. Eine Verbindungsaufnahme über den Gatekeeper durch Eingabe von IP-Adressen ist nicht möglich. Wenn der GWDG-Gatekeeper einen Ruf zu einem Videokonferenzendgerät erhält, welches nicht zu seiner Zone gehört, wird dieser Ruf an den Country-Gatekeeper des DFN-Vereins weitergeleitet, der die Verbindung zu dem angesprochenen Gatekeeper aufbaut. Im Country-Gatekeeper des DFN-Vereins werden alle Gatekeeper des Deutschen Forschungsnetzes registriert, so dass er als einziger allen registrierten Gatekeepern bekannt ist. Über den Country-Gatekeeper kann die MCU und der ISDN-Gateway des DFN-Vereins genutzt werden.

6.3.4 Nutzung der DFN-MCU für Mehrpunktkonferenzen

Die Mehrpunktkonferenzen können jederzeit über das Videokonferenzportal des DFN-Vereins

https://www.vc.dfn.de/konferenz/confid.html

ausgewählt werden, indem entsprechend dem gewünschten Konferenztyp eine Konferenz-ID bezogen wird. Eine tabellarische Auflistung der angebotenen MCU-Dienste wird unter

https://www.vc.dfn.de/doku/technik/mcu-services.html

des in Abschnitt 6.2.5 beschriebenen Videokonferenzportals angeboten.

Die Konferenz wird aufgerufen, indem der Initiator eine Zeichenfolge eingibt, die sich aus der Konferenz-ID und den E.164-Nummern der Teilnehmer, die zur Konferenz eingeladen werden, zusammensetzt. Zwischen der Konferenz-ID und den E.164-Nummern der Teilnehmer sind die Trennzeichen ** zu platzieren (Beispiel: 00491009104888**00495513901543**004955120103434). Die Konferenz-ID wird nach der Benutzung nicht ungültig und kann also wieder verwendet werden. Alternativ können sich alle Teilnehmer separat durch Eingabe der Konferenz-ID an eine vereinbarte Mehrpunktvideokonferenz einwählen.

Es ist unbedingt erforderlich, dass alle Videokonferenzendgeräte vor der Nutzung des Multipoint-Control-Unit-Dienstes an einem Gatekeeper registriert sind, der berechtigt ist, die Dienste des DFN-Vereins zu nutzen.

6.3.5 Nutzung des ISDN-Gateways

Über die beiden ISDN-Gateways des DFN-Vereins können auch H.320-Videokonferenzsysteme (ISDN) an Videokonferenzen über IP teilnehmen. Sind die Videokonferenzsysteme TCS4-fähig, können bei der Einwahl Rufnummer und Konferenz-ID gemeinsam in das Videokonferenzendgerät eingegeben werden.

ISDN-Gateway in Berlin: Tel. 030-25410800

ISDN-Gateway in Stuttgart: Tel. 0711-6330190

Vorgehen ohne TCS4

Für den Verbindungsaufbau wird in das H.320-Videokonferenzsystem eine der beiden ISDN-Gateway-Telefonnummern eingegeben. Nachdem sich eine automatische Ansage gemeldet hat, wird nun die E.164-Nummer des Konferenzpartners oder die Konferenz-ID der MCU-Konferenz sowie ein abschließendes # eingegeben. Nun ist man der Videokonferenz zugeschaltet.

Vorgehen mit TCS4

Für den Verbindungsaufbau wird auch hier eine der beiden ISDN-Gateway-Telefonnummern gefolgt von einem Trennzeichen und der gewünschten E.164-Nummer des Konferenzpartners oder der Konferenz-ID der MCU eingegeben (Beispiel: 07116330190##00495513901543##00495512010 4445). Nun ist man auch hier der Videokonferenz zugeschaltet. Die notwendigen Trennzeichen zwischen Telefonnummer und E.164-Nummer sind nicht bei allen Videokonferenzsystem-Herstellern gleich. Die folgende Tabelle gibt einen Überblick über die bekannten TCS4-Trennzeichen:

Hersteller	Trennzeichen
Polycom	##
Sony	**
Tandberg	*
VCON	^

Körmer

---

7. Kurse des Rechenzentrums

7.1 Allgemeine Informationen zum Kursangebot der GWDG

7.1.1 Teilnehmerkreis

Das Kursangebot der GWDG richtet sich an die Mitarbeiterinnen und Mitarbeiter aus den Instituten der Universität Göttingen und der Max-Planck-Gesellschaft sowie aus anderen wissenschaftlichen Einrichtungen, die zum erweiterten Benutzerkreis der GWDG gehören. Eine Benutzerkennung für die Rechenanlagen der GWDG ist nicht erforderlich.

7.1.2 Anmeldung

Anmeldungen können schriftlich per Brief oder per Fax unter der Nummer 0551 21119 an die

GWDG
Kursanmeldung
Postfach 2841
37018 Göttingen

oder per E-Mail an die Adresse auftrag@gwdg.de mit der Subject-Angabe „Kursanmeldung“ erfolgen. Für die schriftliche Anmeldung steht unter

http://www.gwdg.de/service/nutzung/antragsformulare/kursanmeldung.pdf

ein Formular zur Verfügung. Telefonische Anmeldungen können wegen der Einbeziehung der Kurse in die interne Kosten- und Leistungsrechnung der GWDG nicht angenommen werden. Aus diesem Grund können Anmeldungen auch nur durch den Gruppenmanager - eine der GWDG vom zugehörigen Institut bekannt gegebene und dazu authorisierte Person - oder Geschäftsführenden Direktor des Instituts vorgenommen werden. Die Anmeldefrist endet jeweils 7 Tage vor Kursbeginn. Sollten nach dem Anmeldeschluss noch Teilnehmerplätze frei sein, sind auch noch kurzfristige Anmeldungen in Absprache mit dem Dispatcher (Tel.: 0551 201-1523, E-Mail: auftrag@gwdg.de) möglich. Eine Anmeldebestätigung wird nur an auswärtige Institute oder auf besonderen Wunsch zugesendet. Falls eine Anmeldung wegen Überbelegung des Kurses nicht berücksichtigt werden kann, erfolgt eine Benachrichtigung.

7.1.3 Kosten bzw. Gebühren

Die Kurse sind - wie die meisten anderen Leistungen der GWDG - in das interne Kosten- und Leistungsrechnungssystem der GWDG einbezogen. Die bei den Kursen angegebenen Arbeitseinheiten (AE) werden vom jeweiligen Institutskontingent abgezogen. Für die Institute der Universität Göttingen und der Max-Planck-Gesellschaft erfolgt keine Abrechnung in EUR.

7.1.4 Rücktritt und Kursausfall

Absagen durch die Teilnehmer oder die zugehörigen Gruppenmanager bzw. Geschäftsführenden Direktoren können bis zu 8 Tagen vor Kursbeginn erfolgen. Bei späteren Absagen durch die Teilnehmer oder die zugehörigen Gruppenmanager bzw. Geschäftsführenden Direktoren werden die für die Kurse berechneten Arbeitseinheiten vom jeweiligen Institutskontingent abgebucht. Sollte ein Kurs aus irgendwelchen Gründen, zu denen auch die Unterschreitung der Mindestteilnehmerzahl bei Anmeldeschluss sowie die kurzfristige Erkrankung des Kurshalters gehören, abgesagt werden müssen, so werden wir versuchen, dies den betroffenen Personen rechtzeitig mitzuteilen. Daher sollte bei der Anmeldung auf möglichst vollständige Adressangaben inkl. Telefonnummer und E-Mail-Adresse geachtet werden. Die Berechnung der Arbeitseinheiten entfällt in diesen Fällen selbstverständlich. Weitergehende Ansprüche können jedoch nicht anerkannt werden.

7.1.5 Kursorte

Die meisten Kurse finden in Räumen der GWDG oder des Max-Planck-Instituts für biophysikalische Chemie statt. Der Kursraum und der Vortragsraum der GWDG befinden sich im Turm 6, UG des Max-Planck-Instituts für biophysikalische Chemie, Am Fassberg, 37077 Göttingen, der Große Seminarraum im Allgemeinen Institutsgebäude dieses Instituts. Die Wegbeschreibung zur GWDG bzw. zum Max-Planck-Institut für biophysikalische Chemie sowie der Lageplan sind im WWW unter dem URL

http://www.gwdg.de/gwdg/standort/lageplan

zu finden. Der gemeinsame Schulungsraum von GWDG und SUB befindet sich im Untergeschoss der Niedersächsischen Staats- und Universitätsbibliothek, Platz der Göttinger Sieben 1, 37073 Göttingen.

7.1.6 Ausführliche und aktuelle Informationen

Ausführliche Informationen zu den Kursen, insbesondere zu den Kursinhalten und Räumen, sowie aktuelle kurzfristige Informationen zum Status der Kurse sind im WWW unter dem URL

http://www.gwdg.de/service/kurse

zu finden. Anfragen zu den Kursen können an den Dispatcher per Telefon unter der Nummer 0551 201-1524 oder per E-Mail an die Adresse auftrag@gwdg.de gerichtet werden. Zweimal jährlich wird ein Katalog mit dem aktuellen GWDG-Kursprogramm versendet. Interessenten, die in den Verteiler aufgenommen werden möchten, können dies per E-Mail an die Adresse gwdg@gwdg.de mitteilen.

7.2 Kurse von Juli bis Dezember 2004 in thematischer Übersicht

EDV-Grundlagen und Sonstiges

Kurse	Termine	Vortragende
Einführung in die Nutzung des Leistungsangebots der GWDG	• 15.09.2004 • 08.12.2004	Dr. Grieger Dr. Grieger
Einführung in Aufbau und Funktionsweise von PCs	• 13.09.2004	Eyßell
Führung durch das Rechnermuseum	• 02.07.2004 • 20.08.2004 • 17.09.2004 • 08.10.2004 • 12.11.2004 • 10.12.2004	Eyßell Eyßell Eyßell Eyßell Eyßell Eyßell
Einführung in die Bedienung von Windows-Oberflächen	• 14.09.2004	Eyßell

Betriebssysteme

Kurse	Termine	Vortragende
Grundkurs UNIX/Linux mit Übungen	• 31.08.2004 - 02.09.2004 • 07.12.2004 - 09.12.2004	Hattenbach Hattenbach
Schnellkurs UNIX für Windows-Benutzer mit Übungen	• 05.07.2004 - 06.07.2004 • 29.11.2004 - 30.11.2004	Dr. Bohrer Dr. Bohrer
Installation und Administration von UNIX-Systemen	• 14.12.2004 - 17.12.2004	Dr. Heuer, Dr. Sippel
UNIX für Fortgeschrittene	• 22.11.2004 - 24.11.2004	Dr. Sippel
Die Windows-Active-Directory-Domäne	• 06.10.2004 - 08.10.2004	Quentin
Windows XP für Systembetreuer	• 04.10.2004 - 05.10.2004	Quentin

Netze / Internet

Kurse	Termine	Vortragende
Das Internet als Werkzeug für die Biowissenschaften	• 15.10.2004	Dr. Liesegang
Sicherheit im Internet für Anwender	• 02.12.2004	Reimann
Web Publishing I	• 28.10.2004 - 29.10.2004	Reimann
XML	• 29.09.2004 - 01.10.2004	Reimann, Koch

Grafische Datenverarbeitung

Kurse	Termine	Vortragende
Arbeiten mit CAD, Grundlagen	• 06.09.2004 - 10.09.2004	Witt
CorelDRAW - Grundlagen	• 19.10.2004 - 20.10.2004	Wagenführ
Photoshop für Fortgeschrittene	• 23.08.2004 - 24.08.2004	Töpfer

Sonstige Anwendungssoftware

Kurse	Termine	Vortragende
Datenbanksystem MS Access, Einführung mit Übungen	• 22.11.2004 - 26.11.2004	Dr. Kneser
Anwendungen in Lotus Notes	• 26.10.2004 - 27.10.2004	Greber, Dr. Grieger
PDF-Dateien: Erzeugung und Bearbeitung	• 07.07.2004 - 08.07.2004	Dr. Baier, Koch
PowerPoint	• 21.12.2004 - 22.12.2004	Reimann
Projektplanung mit MS Project	**Neuer Termin!** • 22.07.2004	Reimann
SAS - Grundlagen	• 09.11.2004 - 11.11.2004	Wagenführ
Methoden und Werkzeuge der Sequenzanalyse: GCG, EMBOSS, STADEN	• 11.10.2004 - 14.10.2004	Dr. Bohrer, Dr. Liesegang
Mit StarOffice zum Schwarzen Loch	• 12.11.2004	Dr. Grieger

Programmiersprachen

Kurse	Termine	Vortragende
Einführung in die Programmiersprache Fortran 90/95	• 27.09.2004 - 28.09.2004	Dr. Schwardmann
Programmierung von Parallelrechnern	• 02.11.2004 - 04.11.2004	Prof. Haan, Dr. Schwardmann

7.3 Kurse von Juli bis Dezember 2004 in chronologischer Übersicht

Kurs	Vortragende	Termin	Anmelde-schluss	AE
Führung durch das Rechner-museum	Eyßell	02.07.2004 10.00 - 12.00 Uhr	25.06.2004	0
Schnellkurs UNIX für Windows-Benutzer mit Übungen	Dr. Bohrer	05.07.2004 - 06.07.2004 13.30 - 16.30 Uhr	28.06.2004	4

Kurs	Vortragende	Termin	Anmelde-schluss	AE
PDF-Dateien: Erzeugung und Bear-beitung	Dr. Baier, Koch	07.07.2004 - 08.07.2004 09.15 - 12.00 Uhr und 13.00 - 15.00 Uhr	30.06.2004	8
Projektplanung mit MS Project	Reimann	**Neuer Termin!** 22.07.2004 10.00 - 16.00 Uhr	15.07.2004	4
Führung durch das Rechner-museum	Eyßell	20.08.2004 10.00 - 12.00 Uhr	13.08.2004	0
Photoshop für Fortgeschrittene	Töpfer	23.08.2004 - 24.08.2004 09.30 - 16.00 Uhr	16.08.2004	8
Grundkurs UNIX/Linux mit Übungen	Hattenbach	31.08.2004 - 02.09.2004 09.15 - 12.00 Uhr und 13.30 - 16.00 Uhr	24.08.2004	12
Arbeiten mit CAD, Grundlagen	Witt	06.09.2004 - 10.09.2004 09.00 - 16.00 Uhr, (am 06.09. ab 10.00 Uhr; am 10.09. bis 13.00 Uhr)	30.08.2004	20
Einführung in Aufbau und Funktionsweise von PCs	Eyßell	13.09.2004 09.15 - 12.30 Uhr	06.09.2004	2
Einführung in die Bedienung von Windows-Oberflächen	Eyßell	14.09.2004 09.15 - 12.30 Uhr und 13.30 - 16.00 Uhr	07.09.2004	4
Einführung in die Nutzung des Leistungsangebots der GWDG	Dr. Grieger	15.09.2004 17.15 - 20.00 Uhr	08.09.2004	0
Führung durch das Rechner-museum	Eyßell	17.09.2004 10.00 - 12.00 Uhr	10.09.2004	0
Einführung in die Programmier-sprache Fortran 90/95	Dr. Schwardmann	27.09.2004 - 28.09.2004 09.00 - 12.00 Uhr und 13.00 - 16.00 Uhr	20.09.2004	8
XML	Reimann, Koch	29.09.2004 - 01.10.2004 09.15 - 12.00 Uhr und 13.00 - 15.00 Uhr	22.09.2004	12
Windows XP für Systembetreuer	Quentin	04.10.2004 - 05.10.2004 09.15 - 15.30 Uhr	27.09.2004	8
Die Windows-Active-Directory-Domäne	Quentin	06.10.2004 - 08.10.2004 09.15 - 15.30 Uhr	29.09.2004	12
Führung durch das Rechner-museum	Eyßell	08.10.2004 10.00 - 12.00 Uhr	01.10.2004	0
Methoden und Werkzeuge der Sequenzanalyse: GCG, EMBOSS, STADEN	Dr. Bohrer, Dr. Liesegang	11.10.2004 - 14.10.2004 09.30 - 12.30 Uhr und 13.30 - 16.30 Uhr	04.10.2004	16

Kurs	Vortragende	Termin	Anmelde-schluss	AE
Das Internet als Werkzeug für die Biowissenschaften	Dr. Liesegang	15.10.2004 09.30 - 12.30 Uhr und 13.30 - 16.00 Uhr	08.10.2004	4
CorelDRAW - Grundlagen	Wagenführ	19.10.2004 - 20.10.2004 09.15 - 12.00 Uhr und 13.30 - 16.30 Uhr	12.10.2004	8
Anwendungen in Lotus Notes	Greber, Dr. Grieger	26.10.2004 - 27.10.2004 09.15 - 16.30 Uhr	19.10.2004	8
Web Publishing I	Reimann	28.10.2004 - 29.10.2004 09.15 - 12.00 Uhr und 13.00 - 15.00 Uhr	21.10.2004	8
Programmierung von Parallel-rechnern	Prof. Dr. Haan, Dr. Schwardmann	02.11.2004 - 04.11.2004 09.15 - 12.15 Uhr und 14.00 - 17.00 Uhr	26.10.2004	12
SAS - Grundlagen	Wagenführ	09.11.2004 - 11.11.2004 09.15 - 12.00 Uhr und 13.30 - 16.30 Uhr	02.11.2004	12
Führung durch das Rechner-museum	Eyßell	12.11.2004 10.00 - 12.00 Uhr	05.11.2004	0
Mit StarOffice zum Schwarzen Loch	Dr. Grieger	12.11.2004 09.15 - 12.00 Uhr	05.11.2004	2
Datenbanksystem MS Access, Einführung mit Übungen	Dr. Kneser	22.11.2004 - 26.11.2004 09.00 - 12.00 Uhr	15.11.2004	10
UNIX für Fortgeschrittene	Dr. Sippel	22.11.2004 - 24.11.2004 09.15 - 12.00 Uhr und 13.15 - 15.30 Uhr	15.11.2004	12
Schnellkurs UNIX für Windows-Benutzer mit Übungen	Dr. Bohrer	29.11.2004 - 30.11.2004 13.30 - 16.30 Uhr	22.11.2004	4
Sicherheit im Internet für Anwender	Reimann	02.12.2004 09.15 - 12.00 Uhr und 13.00 - 15.00 Uhr	25.11.2004	4
Grundkurs UNIX/Linux mit Übungen	Hattenbach	07.12.2004 - 09.12.2004 09.15 - 12.00 Uhr und 13.30 - 16.00 Uhr	30.11.2004	12
Einführung in die Nutzung des Leistungsangebots der GWDG	Dr. Grieger	08.12.2004 17.15 - 20.00 Uhr	01.12.2004	0
Führung durch das Rechner-museum	Eyßell	10.12.2004 10.00 - 12.00 Uhr	03.12.2004	0
Installation und Administration von UNIX-Systemen	Dr. Heuer, Dr. Sippel	14.12.2004 - 17.12.2004 09.30 - 12.00 Uhr und 13.30 - 16.30 Uhr	07.12.2004	16
PowerPoint	Reimann	21.12.2004 - 22.12.2004 09.15 - 12.00 Uhr und 13.00 - 15.00 Uhr	14.12.2004	8

8. Betriebsstatistik Mai 2004

8.1 Nutzung der Rechenanlagen

Rechner	Zahl der Prozessoren	CPU-Stunden
DECalpha	12	3.526,54
IBM RS/6000 SP	224	88.360,05
IBM Regatta	96	37.612,14
Linux Parallel	198	132.776,22

8.2 Betriebsunterbrechungen

Rechner/PC-Netz	Störungen		System-pflege	
	Anzahl	Stunden	Anzahl	Stunden
UNIX-Cluster	0		0	
IBM SP/Regatta	0		0	
Linux Parallel	0		0	
PC-Netz	2	4,30	1	12,80
Nameserver	1	0,50	0	
Mailer	2	2.20	1	0,50

9. Autoren dieser Ausgabe

Name	Artikel	E-Mail-Adresse / Telefon-Nr.
Dr. Holger Beck	• Informationsveranstaltung „Sicherheit im GÖNET“ am 29.06.2004 • IT-Sicherheitsleitlinie der GWDG	Holger.Beck@gwdg.de 0551 201-1554
Dr. Christian Boehme	• Einheitliches Batch-System LSF	cboehme@gwdg.de 0551 201-1559
Dr. Wilfried Grieger	• Umbauarbeiten im Rechenzentrum und Konsequenzen für Benutzer • Kontingentzuweisung für das dritte Quartal 2004	wgriege@gwdg.de 0551 201-1512
Thomas Körmer	• Der Videokonferenzdienst des DFN-Vereins und seine Nutzung über den Gatekeeper der GWDG	tkoerme@gwdg.de 0551 201-1555