

Netzwerkweite Datensicherung mit Amanda – Einsatz von Festplatten statt Bändern

7. Juni 2004

Rechtlicher Hinweis

Dieser Beitrag ist lizenziert unter der UVM Lizenz für die freie Nutzung unveränderter Inhalte.

Zusammenfassung

Mit dem Einzug von Linux in allen Bereichen wächst auch die Notwendigkeit, netzwerkweit effizient Daten zu sichern. Selbstgestrickte, skriptbasierte Lösungen mit tar/cpio/dump geraten dann schnell an ihre Grenzen.

Amanda bietet hier eine komfortable Lösung und ist - vom Fehlen eines graphischen GUI mal abgesehen, durchaus zu kommerziellen Lösungen gleichwertig.

Im Vortrag soll im ersten Teil Amanda vorgestellt, Möglichkeiten des Einsatzes erörtert und das Funktionsschema aufgezeigt werden. Nicht zu unterschätzende Features sind etwa die automatische Ermittlung des inkrementellen Levels und die Zwischenspeicherung von "Dumps" damit ist auch eine Datensicherung bei fehlendem Band oder defektem Bandlaufwerk möglich. Das Client-Server Prinzip bietet die Möglichkeit, einen zentralen Backup-Server räumlich getrennt von der Serverfarm aufzustellen (z.B. in einem anderen Brandabschnitt). Im zweiten Teil des Vortrages soll die Möglichkeit vorgestellt werden, statt auf Band auf Festplatten zu sichern. Die Unterschiede und Risiken einer Sicherung auf Festplatte werden diskutiert, anschließend das Funktionsschema aufgezeigt, das auf dem Changer-Mechanismus aufbaut und identisch zu Tape-Changern funktioniert. Eine konkrete, detaillierte Konfiguration bietet der Vortrag nicht, dafür reicht die Zeit von 45 min (+15 min Diskussion). Dafür soll aber eine konkrete Konfiguration für die Sicherung auf Festplatte mit Kurzanleitung als Anhang zum Paper (oder per Download im Internet) zur Verfügung gestellt werden.

1 Allgemeines zur Datensicherung

Primäres Ziel einer jeden Datensicherung ist die Wiederherstellung von Daten, die verloren gegangen sind. Die Datensicherung ist ein „Fallback“, eine Alternativ-Strategie, um die Verfügbarkeit von Daten sicherzustellen. Käme es generell zu keinem Datenverlust, bräuchte man auch keine Alternativ-Strategie, um verloren gegangene Daten wieder herzustellen. Im Falle eines Datenverlustes im Primärsystem (zum Beispiel Festplattenausfall am Fileserver) ist es ganz entscheidend, daß jetzt die Alternativstrategie zur Sicherung der Verfügbarkeit der Daten funktioniert. Die Ursache, die zum Verlust der Daten geführt hat, darf also keinesfalls auch gleichzeitig zum Verlust der Alternativ-Strategie führen. Ein Punkt, der leider immer wieder nicht bedacht und vernachlässigt wird.

Im nachfolgenden wird daher auf die Frage „was führt zu einem Datenverlust“ eingegangen (Gefährdungsarten) und daraus Anforderungen an eine Datensicherung abgeleitet. Auf dieser Basis werden die Vor- und Nachteile einer Datensicherung auf Festplatte statt auch Wechselmedien wie Bändern diskutiert.

1.1 Gefährdungsarten

- *Äußere Einflüsse, Höhere Gewalt* : Feuer, Wasser oder Blitzeinschlag (Überspannung) betreffen selten ein einzelnes Hardwarebauteil, sondern mindestens den gesamten Rechner, oft aber auch einen ganzen Raum oder den gesamten Brandabschnitt.

- *Menschliches Versagen oder Vorsatz* : Versehentliches Löschen eigener, meist einzelner Dateien oder Verzeichnisse durch den Anwender oder fehlerhafte Anwendung von kritischen Befehlen (fsck im laufenden Betrieb) durch den Administrator. Sabotage durch „gekündigte Mitarbeiter oder interne/externe Hacker.
- *Technisches Versagen* : Ausfall von Festplatten oder anderen Hardware-Komponenten oder etwa fehlerhafte Datenträger.

1.2 Anforderungen an eine Datensicherung

- *Räumliche Trennung* zwischen Original und Sicherung: Befindet sich das Sicherungsmedium im gleichen Raum oder vielleicht sogar im gleichen Rechner, ist die Sicherung genauso gefährdet wie die Originaldaten (höher Gewalt, technisches Versagen).
- *Regelmäßige Sicherung* , am besten automatisiert.
- *Historische Sicherung* : Bemerkt ein Anwender das Löschen einer Datei erst Tage später, ist diese bei täglicher Sicherung nicht mehr in der aktuellen Sicherung enthalten. Gibt es mehrere Versionen der Datensicherung (z.B. tägliche Sicherung aus den letzten Tagen) wächst die Wahrscheinlichkeit, die verloren gegangenen Daten doch noch herstellen zu können.
- *Wiederherstellung vollständiger Systeme* (nach technischem Defekt)
- *Einfaches, gezieltes Wiederauffinden* einzelner Dateien für die Rücksicherung

1.3 Sicherungsmedium: Band oder Festplatte?

Stark fallende Preise und riesige Kapazitäten gerade bei Festplatten im günstigen ATA-Bereich lassen immer öfter die Frage aufkommen, warum man nicht statt wie bisher auf Band gleich auf eine Festplatte sichern sollte.

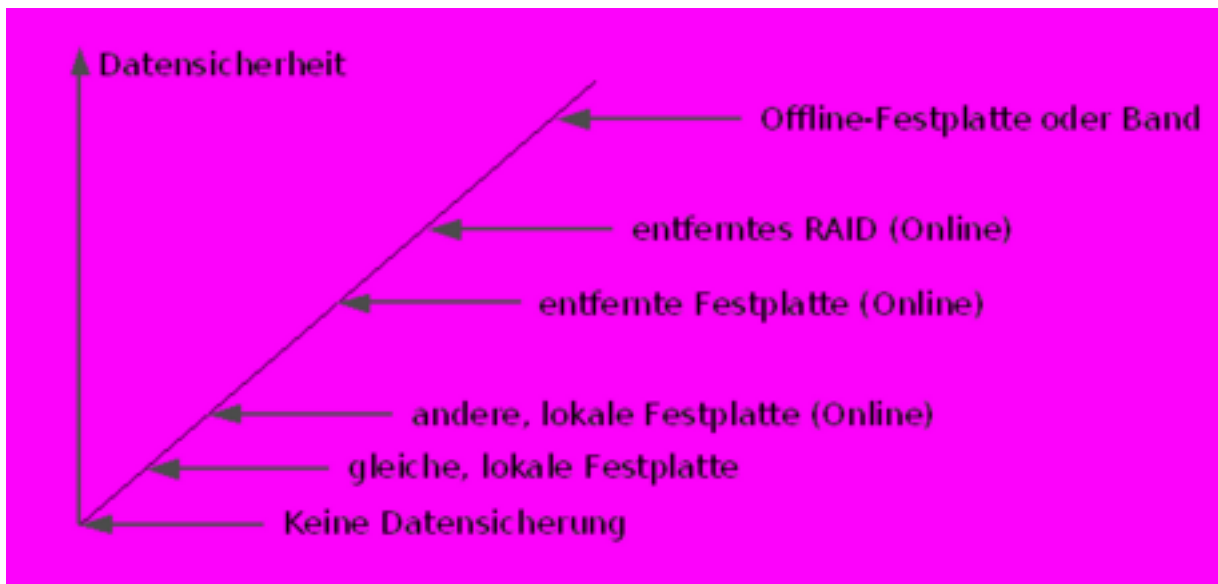
Sofern man Festplatten als Sicherungsmedium nicht als Wechselplatte einsetzt, ist die Platte in der Regel immer Online. Man kann die Festplatte zwar in einem System unterbringen, das räumlich getrennt (mindestens ein anderer Brandabschnitt) vom Fileserver steht, allerdings bleibt die Gefährdung durch Überspannungen. Ein „Offline“-Sicherungsmedium wie ein Band, sicher verwahrt in einem feuerfesten Tresor in räumlicher Entfernung vom Fileserver bietet eine wesentlich höhere Sicherheit.

Gegen technisches Versagen (Ausfall der Festplatte) kann und sollte man RAID einsetzen. Um eine Historie der Datensicherung bereit zu stellen, sind entsprechende Kapazitäten erforderlich. Beispiel: eine durchschnittliche Datensicherung benötigt 20 GByte, es sollen 10 Versionen vorgehalten werden, dann sind 200 GByte Gesamtkapazität notwendig. Achtung: Bei Online-Systemen, bei denen die Historie in Verzeichnissen eines einzigen RAID-Systemes untergebracht wird, besteht allerdings die Gefahr, durch eine Fehlbedienung (menschliches Versagen) gleich alle Versionen der Sicherung zu zerstören.

Im Prinzip kann man Festplatten auch als Offline-Medien einsetzen. Sofern die Technologie Hotplugging erlaubt und der Server entsprechend ausgestattet ist, lassen sich auch Festplatten wie andere Wechselmedien nur zur Sicherung einlegen und nach der Sicherung offline in einem feuerfesten Tresor verwahren. Allerdings muß man berücksichtigen, daß die Lebensdauer der Festplatte durch unregelmäßiges Einschalten und den Transport beeinträchtigt werden kann.

Macht man sich die Besonderheiten einer Sicherung auf Festplatte bewußt, ist es abhängig von Sicherheitsanforderungen und Budget in verschiedenen Fällen durchaus sinnvoll und möglich, eine Sicherung auf Festplatte vorzunehmen.

Die nachstehende Graphik zeigt schematisch den Grad der Datensicherheit abhängig von der eingesetzten Sicherungsvariante.



2 Amanda: eine Einführung

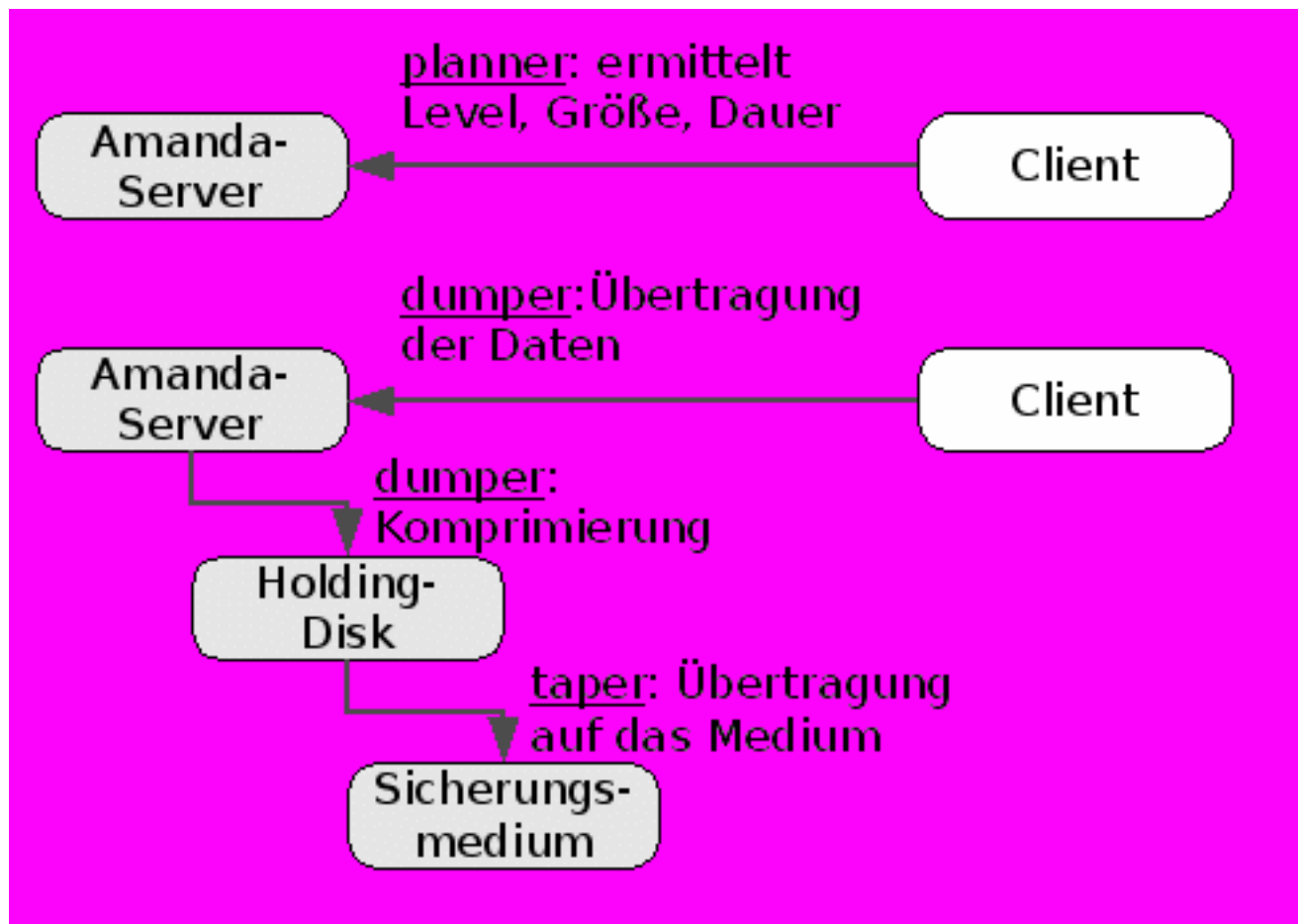
Solange man nur ein oder zwei Rechner zu sichern hat, lässt sich die Datensicherung recht überschaubar mit Boardmitteln wie tar oder rsync bewerkstelligen. Für eine größere Anzahl von Systemen bietet sich Amanda an, der „Advanced Maryland Automatic Network Disk Archiver“ (www.amanda.org <<http://www.amanda.org/>>). Ursprünglich für die Sicherung auf Bändern gedacht, ist inzwischen auch eine Sicherung auf Festplatte möglich. Die Konfiguration für eine Sicherung auf Festplatte unterscheidet sich fast nicht von einer Sicherung auf Band. Der Wechsel ist daher nicht schwierig, man kann ohne weiteres auch eine gemischte Sicherung durchführen, etwa die tägliche Sicherung auf Disk, und eine monatliche Vollsicherung zu Archivierungszwecken auf Band. Zum besseren Verständnis sollen zunächst die grundlegenden Eigenschaften von Amanda vorgestellt werden, eine Konfiguration wird dann anhand einer Sicherung auf Festplatte beschrieben.

2.1 Eigenschaften von Amanda

- *Client-Server-Architektur:* Auf dem Client wird ein Daemon (per Inetd) installiert (die Installation eines Amanda-Paketes aus der Linux-Distribution ist meist ausreichend). Der Sicherungsserver kontaktiert den Client-Daemon und ruft neben den Daten auch statistische Informationen ab.
- *Standard-Format:* Zur Sicherung wird GNU-Tar oder dump eingesetzt, das entsprechende Archivformat (ergänzt um einen Amanda-spezifischen Header) findet sich auch auf den Sicherungsmedien wieder. Bei Verwendung von GNU-Tar können auch einzelne Verzeichnisse gesichert und Include/Exclude-Pattern verwendet werden.
- *Auto-Inkrementelle Sicherung:* Der Sicherungslevel bei einer inkrementellen Sicherung wird automatisch bestimmt und optimiert. Benötigt ein niedrigerer inkrementeller Level nur wenig mehr Speicherplatz als der aktuell geplante Level, wird im niedrigeren Level gesichert, damit sinkt die Anzahl der erforderlichen Bänder bei einer Rücksicherung.
- *Holding Disk:* Die Holding Disk ist ein Zwischenspeicher, in dem die laufenden Sicherungen abgelegt werden können, bevor diese auf das Sicherungsmedium geschrieben werden. Bei Bändern erlaubt das maximale Schreibgeschwindigkeit der bereits vorbereiteten Sicherungen, außerdem ermöglicht die Holding Disk eine parallele Sicherung vieler Clients. Ist das Sicherungsmedium nicht verfügbar (z.B. Band nicht eingelegt), wird die Sicherung trotzdem durchgeführt, die Daten in der Holding Disk gespeichert und können später nachträglich auf das Sicherungsmedium geschrieben werden. Bei einer klassischen Sicherung wird die ganze Sicherung abgebrochen (nicht gesichert), wenn das Sicherungsmedium nicht verfügbar ist.

- *Bandverwaltung*: Registrierte Bandlabels erlauben die Identifikation eines bestimmten Bandes und verhindern versehentliches Überschreiben.
- *Indexverwaltung*: Einzelne Dateien oder Verzeichnisse können gezielt restauriert werden.
- *Software-Komprimierung*: Amanda ermöglicht eine software-seitige Komprimierung mit vielen Auswahlmöglichkeiten (Server- oder Client-seitige Komprimierung, Optimierung auf Geschwindigkeit oder maximale Kompression).
- *Health Check*: Das Programm amcheck erlaubt eine Überprüfung der Datensicherung vor dem eigentlichen Sicherungslauf.
- *Email-Benachrichtigung*: Nach erfolgter Datensicherung berichtet Amanda ausführlich über Erfolg/Mißerfolg, aufgetretene Probleme und verschiedenen Statistiken in einer zusammenfassenden Email.
- *Unterstützung für RAIT*: „Redundant Array of Independend Tapes“: Sicherung auf mehreren Bändern mit Checksummen (Kapazität N-1, Verfahren vergleichbar mit RAID-5).
- *Werkzeuge zur Administration*: Verschiedene Programme zur Administration geben Auskunft über geplante Vollsicherungen, unterschiedliche Statistiken und welche Sicherung sich auf welchem Band befindet.

2.2 Funktionsschema



Die Abbildung zeigt das grobe Funktionsschema von Amanda. Zunächst ermittelt das Programm planner für

jede zu sichernde „Disk“ (Verzeichnis oder Filesystem) den inkrementellen Level, die ungefähr zu sichernde Größe und die geschätzte, benötigte Zeit. Der Vorgang erfolgt parallel für alle Clients. Die Übertragung der Daten von den Clients zum Server übernimmt das Programm dumper, der Vorgang kann beim Einsatz einer Holding Disk ebenfalls parallel erfolgen (in der Regel eine Sicherung je Client gleichzeitig, abhängig von der Konfiguration). Für das Schreiben auf das Sicherungsmedium ist taper zuständig. Durch den Einsatz unterschiedlicher Output-Treiber kann das Medium ein Band, ein RAIT oder ein Verzeichnis sein.

3 Amanda: Sicherung auf Festplatten

Nach der einführenden Diskussion um Gefährdungsarten und Anforderungen an eine Datensicherung sollte es selbstverständlich sein, daß der Sicherungsserver räumlich getrennt von den zu sichernden Daten stehen sollte - mindestens in einem anderen Brandabschnitt (bei Einsatz von SAN-Technologien gilt das natürlich in erster Linie für den eigentlichen Storage, da hier Storage und Sicherungsserver räumlich nicht aneinander gebunden sind).

Mit Amanda lassen sich mehrere Sicherungsläufe parallel definieren. Ein Sicherungslauf ist ein Satz von Datensicherungen, die gleichzeitig zusammen gesichert und auf dasselbe Sicherungsmedium weggeschrieben werden. So lassen sich etwa mehrere Sicherungsläufe gleichzeitig durchführen, wenn die Sicherungsmedien parallel bedient werden können, etwa wenn für jeden Sicherungslauf ein eigenes Bandlaufwerk zur Verfügung steht.

Zur Unterscheidung bekommt jeder Sicherungslauf einen eigenen Namen und seine eigenen Verzeichnisse für Konfiguration, Datenbank und Holding Disk. Die Bezeichnung für den nachstehend beschriebenen Sicherungslauf ist „std“.

3.1 Konfiguration

Verzeichnisstruktur für Konfiguration, Datenbank und Holding Disk:

```
/etc/amanda/std          # Konfiguration
/data/amandadump/std     # Holding Disk
/var/lib/amanda/std/log  # Logfiles
/var/lib/amanda/std/info # Info-Datenbank
/var/lib/amanda/std/index # Indexverwaltung
```

Der File-Output-Treiber schreibt in ein Verzeichnis, in unserem Beispiel simuliert Amanda einen Tape-Changer über eine Verzeichnisstruktur, mehrere Sicherungsmedien werden als Slots in Form von Unterverzeichnissen dargestellt.

Benötigt wird eine ausreichend große Festplatte, besser ein RAID-System. Angenommen, eine Vollsicherung aller Clients ist ca. 20 GByte groß, es sollen 5 Versionen der Sicherung vorgehalten werden, dann sollte der zur Verfügung stehende Plattenplatz mindestens 100 GByte betragen (beim Einsatz von Wechselfestplatten eben mindestens 20 GByte je Wechselplatte).

Die Verzeichnisstruktur für die Sicherung ist:

```
/data/vtapes/std        # Hauptverzeichnis
/data/vtapes/std/info   # Info-Datei
/data/vtapes/std/slot1  # erstes virtuelles Tape (Verzeichnis)
...
/data/vtapes/std/slotn  # letztes virtuelles Tape
/data/vtapes/std/data   # Symlink auf aktuelles virtuelles Tape
```

Bei 5 Sicherungen kommen die Verzeichnisse slot1 ... slot5 zum Einsatz. Der Symlink „data“ zeigt jeweils auf das aktuelle Verzeichnis, er wird vom Changer-Mechanismus (zum Einsatz kommt das Skript „chg-disk“)

entsprechend umgesetzt. Bei einer Offline-Sicherung auf Wechselfestplatten kann man die jeweilige Sicherungsplatte auch direkt unter „data“ mounten.

Alle Verzeichnisse, ob Konfiguration, Datenbank, Holding Disk oder Sicherungsdisk müssen für den Amanda-User schreibbar sein („backup“ bei Debian, „amanda“ bei SuSE). Die Verzeichnisse, die Daten enthalten (Holding Disk, Sicherungsdisk), sollten natürlich nur für den Amanda-User lesbar sein!

Das eigentliche Konfigurationsfile heißt immer „amanda.conf“ und liegt im Konfigurationsverzeichnis des Sicherungslaufes, hier „/etc/amanda/std“.

```
#
# /etc/amanda/std/amanda.conf
#
org "std"
#
mailto "wob@swobspace.de"
tapedev "file:/data/vtapes/std"
labelstr "^std-[0-9]+$"
tapetype HARDDISK
tpchanger "chg-disk"
changerfile "/etc/amanda/std/changer"
#
diskfile "disklist"
infofile "/var/lib/amanda/std/info"
indexdir "/var/lib/amanda/std/index"
logdir "/var/lib/amanda/std/log"
tapelist "tapelist"
#
dumpcycle 7
runspercycle 5
tapecycle 5
#
define dumptype normal {
    comment "Normal backup"
    program "GNUTAR"
    compress server fast
    index yes
}
#
define tapetype HARDDISK {
    comment "Dump to disk (vtape)"
    length 20000 mbytes
}
#
define interface eth0 {
    comment "100 Mbps ethernet"
    use 800 kbps
}
#
holdingdisk hd1 {
    comment "main holding disk"
    directory "/data/amandadump/std"
    use -4 Gb
    chunksize 1Gb
}
#
```

reserve 50

Die Parameter im Einzelnen: „org“ ist ein Bezeichner, der unter anderem in den Infomails verwendet wird. Sinnvollerweise ist dieser identisch mit dem Namen des Sicherungslaufes. Die Mails, die Amanda versendet, gehen an „mailto“. Um eine Verwechslung der Sicherungsmedien zu verhindern, kann der Label, den das Medium erhält, eingeschränkt werden. Mit „labelstr“ wird ein Pattern festgelegt, das die erlaubten Labels beschreibt.

„tapedev“ gibt den Output-Treiber und das Output-Device an, hier soll der File-Treiber verwendet werden, das Verzeichnis „/data/vtapes/std“ beschreibt das Rootverzeichnis der virtuellen Tapes. „tapetype“ gibt den Typ an, unter „define tapetype“ sind die Parameter zu finden, außer einem Kommentar wird dort nur die Angabe der maximalen zur Verfügung stehenden Größe an Sicherungskapazität je Lauf angegeben. „tpchanger“ beschreibt das Changer-Skript, hier wurde das bei Amanda mitgelieferte Skript „chg-disk“ verwendet. Das Skript sorgt für den Wechsel der virtuellen Tapes (u.a. Umsetzen des Symlinks). „changerfile“ ist ein Prefix für Parameter, die das Changer-Skript sich merkt.

Hinter „diskfile“ verbirgt sich eine Datei, die beschreibt, was wie gesichert werden soll. Wir gehen gleich noch näher darauf ein. „tapelist“ beinhaltet die für den Sicherungslauf bekannten Bänder (werden beim Labeln dort eingetragen). Die Datei muß existieren (anlegen mit „touch tapelist“) und für den Amanda-User schreibbar sein.

Wie oft gesichert werden soll, beschreibt „dumpcycle“. Hier ist das Intervall 7 Tage, alle 7 Tage wird mindestens eine Vollsicherung gefahren. „runspcycle“ gibt an, daß je dumpcycle nur 5 Läufe stattfinden (Intervall ist eine Woche, die Sicherung findet aber nur werktags statt). „tapecycle“ beschreibt die Anzahl der verfügbaren Medien. Wurden „tapecycle“ Medien benutzt, darf das erste Medium wieder überschrieben werden.

„define dumptype“ definiert Parameter für die Sicherung. Hier wird GNU-Tar verwendet (statt DUMP für dump), die Kompression soll erst am Server stattfinden, die Indexverwaltung für gezieltes Recovery wird eingeschaltet.

Mit „define interface“ wird ein logisches Interface beschrieben, das eigentlich nichts mit dem physikalischen Interface zu tun hat. Die Bandbreite benutzt Amanda nur für eine Kalkulation, ob weitere Clients parallel angesprochen werden können oder ob eine weitere, parallele Sicherung eines Clients aufgrund einer Bandbreitenüberschreitung zurückgestellt wird. Eine echte Beschränkung als Obergrenze für die maximal verwendbare Bandbreite ist gibt es jedoch nicht.

Der „holding disk“ Parameter enthält das Verzeichnis und eine Angabe, wieviel Platz dort verwendet werden darf, hier ist das alles bis auf 4 GByte. Schließlich gibt der Parameter „reserve“ an, daß 50% der Holding Disk für inkrementelle Backups reserviert sind. Ist das Sicherungsmedium nicht verfügbar, schaltet Amanda automatisch auf inkrementelle Backups um, falls nicht mehr ausreichend Platz in der Holding Disk zur Verfügung steht, auch wenn eigentlich ein Vollbackup gefahren werden müßte.

3.1.1 Was wird gesichert: /etc/amanda/std/disklist

```
#
# /etc/amanda/std/disklist
#
# host disk dumptype spindle interface
client1 /      normal  -1  eth0
client1 /usr   normal  -1  eth0
client1 /var   normal  -1  eth0
client1 /data  normal  -1  eth0
#
client2 /data  normal  -1  eth0
#
client3 /data  normal  -1  eth0
```

Das diskfile „disklist“ („disklist“ ist der Default-Name der Datei) beschreibt, welche „Disks“ (bei Verwendung von GNU Tar sind das immer Verzeichnisse) auf welchen Rechnern gesichert werden sollen. Der Dum-

ptype „normal“ wurde in amanda.conf bereits definiert. Alle Disks mit demselben Spindle werden nacheinander - nie gleichzeitig - gesichert. Steht dort -1, wird darauf keine Rücksicht genommen (wieviele gleichzeitig gesichert werden, hängt dann von den Parametern „maxdumps“ und „inparallel“ ab - siehe „man amanda“). Das Interface kann man hier auch weglassen, allerdings käme dann die Default-Einstellung zum Tragen: es würde das Interface „local“ verwendet, das - falls nicht anders definiert - auf eine Bandbreite von 300 kBytes/sec. voreingestellt ist (etwas wenig für aktuelle High-Speed-Netzwerke).

3.1.2 Konfiguration des inetd: /etc/inetd.conf

```
amanda dgram udp wait backup /usr/lib/amanda/amandad amandad
amandaidx stream tcp nowait backup \
  /usr/lib/amanda/amindexd amindexd
amidxtape stream tcp nowait backup \
  /usr/lib/amanda/amidxtaped amidxtaped
```

Die erste Zeile ist für jeden Client erforderlich (der Server ist auch ein Client, wenn er sich selbst sichert), Zeile 2 und 3 sind nur am Server erforderlich. Nach dem Editieren nicht vergessen, den Inetd zum Reload der Konfiguration zu veranlassen (oder neu starten).

3.2 Initialisierung

Sind alle notwendigen Verzeichnisse und die beiden Konfigurationsdateien („amanda.conf“ und „disklist“) angelegt, müssen die virtuellen Tapes (die Unterverzeichnisse mit dem Namen slot1 .. slot5 „gelabelt“ werden:

```
% amlabel std std-001 slot 1
% amlabel std std-002 slot 2
% amlabel std std-003 slot 3
% amlabel std std-004 slot 4
% amlabel std std-005 slot 5
```

„std“ ist die Bezeichnung des Sicherungslaufes, alle Amanda-Kommandos benötigen diese Angabe, um die korrekte Konfigurationsdateien und Datenbankverzeichnisse referenzieren zu können. „std-001“ ist ein Label gemäß der Pattern-Spezifikation „labelstr“. Da ein Tape-Changer simuliert wird, folgt zusätzlich die Angabe der Slot-Nummer.

3.3 Durchführung der Sicherung

Vor der eigentlichen Sicherung testet man die Konfiguration mit dem Programm amcheck. Später kann man das Programm per cron während der Bürozeiten vor einer Sicherung laufen lassen, um gegebenenfalls auftretende Problem noch vor Dienstschluß (und vor der automatischen Sicherung) beheben zu können. Hier eine Beispielausgabe für eine korrekte Funktionsweise:

```
% amcheck std
Amanda Tape Server Host Check
-----
Holding disk /data/amandadump/std: 36215420 KB disk space available, using 32021116 KB
amcheck-server: slot 2: date 20040425 label std-002 (active tape)
amcheck-server: slot 3: date X          label std-003 (new tape)
NOTE: skipping tape-writable test
Tape std-003 label ok
```

Server check took 0.550 seconds

Amanda Backup Client Hosts Check

Client check: 1 host checked in 10.195 seconds, 0 problems found
(brought to you by Amanda 2.4.5b1-20040423)

Hier verweist im Moment noch der Symlink data auf slot2 (das vtape std-002), amcheck (oder auch ein Aufruf von amdump) korrigiert das sofort. Ein zweiter Aufruf zeigt dann nur noch die Zeile mit std-003, auf das letztenendes hier gesichert wird.

Die Sicherung selbst erfolgt mit amdump:

```
% amdump std
```

Die Angabe des Sicherungslaufes (hier „std“) ist zwingend erforderlich. Nach erfolgter Sicherung sendet Amanda eine Mail mit Infos und der Zusammenfassung an die Mailadresse unter „mailto“.

3.4 Recovery

Für die Rücksicherung gibt es zwei Programme:

- *amrestore* : liefert die Sicherung in dem Format des verwendeten Archivprogrammes, also einfaches Tar-Format bei GNU-Tar. Sinnvoll für einen Full-Restore, insbesondere bei gleichzeitigem Restore von mehreren Rechnern. Etwas aufwendiger in der Anwendung.
- *amrecover* : interaktives Programm, benötigt eingeschaltetes Indexing, einzelne Dateien oder Verzeichnisse lassen sich komfortabel rücksichern. Ideal für den täglichen Gebrauch bei Userfehlern.

3.4.1 Beispiel für amrecover

Ein interaktiver Restore über amrecover muß als Root ausgeführt werden, um die Eigentümerschaft und Zugriffsrechte der zurückgesicherten Dateien korrekt abzubilden. Im nachfolgenden Beispiel wird in ein eigenes Extrakt-Verzeichnis gewechselt, um nicht versehentlich die existierenden Daten zu überschreiben. Dann wird das Verzeichnis /etc/amanda zurückgesichert, das sich auf der Disk „/“ befindet (siehe Einträge in „disklist“).

```
% mkdir /var/restore  
% cd /var/restore  
% amrecover std
```

```
AMRECOVER Version 2.4.5b1-20040423. Contacting server on localhost ...  
220 swobspace AMANDA index server (2.4.5b1-20040423) ready.  
200 Access OK  
Setting restore date to today (2004-04-28)  
200 Working date set to 2004-04-28.  
Scanning /data/amandadump/std...  
  20040427220022: found Amanda directory.  
200 Config set to std.  
200 Dump host set to swobspace.  
Trying disk /var ...  
$CWD '/var/restore' is on disk '/var' mounted at '/var'.  
200 Disk set to /var.  
Invalid directory - /var/restore
```

```
amrecover> setdisk /
```

```
200 Disk set to /.  
amrecover> cd /etc/  
/etc
```

```
amrecover> add amanda
```

```
Added dir /etc/amanda at date 2004-04-25
```

```
amrecover> extract
```

```
Extracting files using tape drive file:/data/amvtape/std on host localhost.  
The following tapes are needed: std-002
```

Hier wird das korrekte Band gefordert. In der Regel steht der virtuelle Tapechanger gerade an einer anderen Stelle. Am einfachsten benutzt man das Changer-Skript für den Slotwechsel, allerdings muß das aus dem Konfigurationsverzeichnis heraus aufgerufen werden (zweckmäßigerweise von einem anderen Terminalfenster aus):

```
% cd /etc/amanda/std  
% /usr/lib/amanda/chg-disk -slot 2
```

Jetzt kann man mit dem Recovery fortfahren:

```
Restoring files into directory /var/restore
```

```
Continue [?/Y/n]? y
```

```
Extracting files using tape drive file:/data/amvtape/std on host localhost.  
Load tape std-002 now
```

```
Continue [?/Y/n/s/t]? y  
./etc/amanda/
```

```
...
```

```
amrecover> exit
```

Die zurückgesicherten Dateien befinden sich jetzt im Verzeichnis

```
/var/restore/etc/amanda
```

3.5 Quellenhinweise

Die kurze Darstellung von Amanda kann natürlich nicht auf alle Aspekte eingehen. Folgende Quellenhinweise sollten weitere, nützliche Informationen im Umgang mit Amanda liefern:

- Wolfgang Barth: Datensicherung unter Linux; Open Source Press 2004
- HOWTO-FILE-DRIVER von Stefan G. Weichinger im ./docs-Verzeichnis der Source-Distribution) und andere dort vorhandene Dokumente
- `man amanda` (vollständige Beschreibung des Konfigurationsfiles
- <http://www.backupcentral.com/amanda.html> <<http://www.backupcentral.com/amanda.html>> (englisch): Kapitel aus „Unix Backup & Recovery“, O'Reilly (ebenfalls englisch).