Sicherheit unter Linux

Mark Heisterkamp

19. Juni 2006

Daten- und Systemsicherung, Archivierung

Es gibt drei unterschiedliche Bereiche:

- Datensicherung
- Datenarchivierung
- Systemsicherung

Datensicherung (Backup)

- unverzichtbarer Service für den Nutzer
- wird im Allgemeinen vom Nutzer als verzichtbar eingestuft
- viele Nutzer sind erfahrungsresistent
- kurzfristiger Service
- inkrementelles Backup mit „Gedächtnis“ ist wünschenswert

lokale Backup-Medien

CD, DVD	Nicht zur Archivierung, aber als kurzfristiges Backup gut geeignet. Nur sehr begrenzte Speicherkapazität.
USB-Stick	Einfache Speicherung, sehr begrenze Kapzität, ansonsten siehe CD und DVD.
Band	Teure und seltene Geräte, zur Archivierung geeignet, sehr langsam aber relativ hohe Kapazität.
2. Festplatte	Schnell, hohe Kapazität, aber keine räumliche Trennung von Original und Backup möglich (gilt nicht für externe Platten).
Notebook	Schnell, hohe Kapazität, teuer und unhandlich.
Diskette	Höchst unzuverlässiges Medium, viel zu wenig Kapazität.

Backup im Netz - E-Mail

Schicken Sie einfach wichtige Daten regelmäßig als Anhang per E-Mail an sich selbst.

Vorteile:

- einfach
- zuverlässig
- hohe Verfügbarkeit
- hohe Datensicherheit

Nachteile:

- Anhänge vielleicht zu groß?
- gute Netzanbindung erforderlich
- begrenzte Kapazität der Mailbox
- kein Automatismus
- Eigenverantwortlichleit

Backup im Netz - Unix-Tools

Sichern Sie Daten mit Unix-Tools auf im Netz erreichbare Rechner.

Vorteile:

- Eigenverantwortlichkeit
- hohe Zuverlässigkeit
- mit Bordmitteln machbar
- Verschlüsselung

Nachteile:

- Eigenverantwortlichkeit
- Finde ich taugliche Zielrechner?
- gute Unix-Kenntnisse erforderlich

Backup im Netz - Unix-Tools

Einige Tools:

- `ssh` (mit Public-Key-Authentifizierung zur Automatisierung)
- `ftp` (mit `.netrc` zur Automatisierung)
- `netcat` (`nc`)
- `tar`
- `rsync`
- `scp`
- `cp`

Beispiele

`ftp:> put "| tar cf - <Quelle>" archiv.tar` und
`ftp:> get test.tar "| tar xf - -C <Ziel>"`

```
cat archiv.tar | ssh <ID>@<Host> "tar xf - -C <Ziel>"
```

Zielrechner (Host): `nc -l -p <Port> > archiv.tar`
Quellrechner: `tar cf - <Quelle> | nc -w 2 <Host> <Port>`

```
rsync -av -e "ssh" <Quelle> <ID>@<Host>:<Ziel>
```

Backup im Netz - Netzlaufwerke

Sichern Sie Ihre Daten per „Copy & Paste“ auf einem Fileserver (Samba, Novell, NFS...).

Vorteile:

- hohe Geschwindigkeit
- hohe Kapazität
- hohe Datensicherheit

Nachteile:

- Eigenverantwortlichkeit
- unverschlüsselt

Backup im Netz - Backupservices

Nehmen Sie an einem Backupservice eines Dienstleisters teil.

Vorteile:

- automatisiert
- zuverlässig
- ggf. einfache Bedienung
- für die meisten Betriebssysteme erhältlich
- hohe Geschwindigkeit
- inkrementell

Nachteile:

- Aufgabe der Eigenverantwortlichkeit
- gute Netzanbindung erforderlich

Backup im Netz - Veritas am RRZN

Ansprechpartner am RRZN:

Christian Otto
otto@rrzn.uni-hannover.de

Rüdiger Rode
rode@rrzn.uni-hannover.de

Ansgar Giesker
giesker@rrzn.uni-hannover.de

Datenarchivierung

- nicht zum kurzfristigen Wiederherstellen von Daten
- nur zur Archivierung
- langfristig
- ggf. teuer
- ggf. sehr aufwendig
- langsam
- große Kapazität notwendig

Medien

- Band (mit Roboter in großen Netzen)
- CD, DVD
- `asterix.rrzn.uni-hannover.de`

Alle Medien müssen regelmäßig umkopiert werden, um Datenverlust vorzubeugen und die Kompatibilität (Lesbarkeit) der Formate und Medien über einen langen Zeitraum zu gewährleisten.

Systemsicherung (Systemrecovery)

- das System wird gesichert
- Separation in Nutzer- und Systemdaten
- schnelles Recovery
- handhabbare Bootmedien
- mit Bordmitteln unter Linux machbar

Methoden

- Platten klonen:
  `dd`
- tar-Archive:
  `dd`
  `sfdisk`
  `tar`
  `chroot`
  `grub-install`

Klonen mit dd

- booten mit Knoppix o. Ä.
- Netzwerk initialisieren
- Plattenressource einhängen (NFS, `netcat`, `ssh...`)
- `dd if=/dev/<SYSTEMPLATTE> of=<PLATTENRESSOURCE>`

Das erzeugte Image ist eine 1:1-Kopie der Systemplatte. Mittels

`dd if=<PLATTENRESSOURCE> of=/dev/<NEUE_SYSTEMPLATTE>`

kann der System-Klon aufgesetzt werden.

Recovery mit tar

System-Image erzeugen:

- Boot von Knoppix o. Ä.
- Dump des Bootsektors der Platte (hda):
  ```
  dd if=/dev/hda bs=512 count=1 of=mbr.hda.dd
  ```
- Dump der Partitionierung:
  ```
  sfdisk -d /dev/hda > sfdisk.txt
  ```
- Einhängen des Systems des System-Dateibaums (z. B. nach `/mnt`
- `tar`-Archiv des Systems erzeugen
  ```
  tar cvzf system.tgz /mnt
  ```

Recovery mit tar

System-Image zurückspielen:

- Platte Partitionieren:
  `sfdisk -f /dev/hda < sfdisk.txt`
- Partionen formatieren:
  `mkfs ...`
- Master-Boot-Record einpsielen:
  `dd if=mbr.hda.dd of=/dev/hda`
- Platte einhängen (z. B. nach `/mnt`)
- `tar`-Archiv entpacken:
  `tar xvzf system.tgz -C /mnt`
- ggf. (je nach grub-Version) Bootloader aktualisieren:
  `chroot /mnt`
  `grub-install /dev/hda`

Funkvernetzung

Das WLAN ist seit einigen Jahren an der Uni flächendeckend vorhanden.

Zugang haben:

- Studierende mit einem Account bei der Unix-AG
- MitarbeiterInnen mit Terminalserver-Zugang (ORG.BEN 28)
- TeilnehmerInnen an Projekten von Einrichtungen an der Uni
- ggf. TeilnehmerInnen an Tagungen o. Ä.

WLAN-Topografie

Gebäude	Bezeichnung	Geschoss	APs	Bemerkungen
1101	Welfengarten	SG	3	Betrieb
			4	Betrieb
		Außenbereich	3	Betrieb
		Lichthof	4	Betrieb
		AudiMax	4	Betrieb
		Gr. Physiksaal	3	Betrieb
		Hörsaal F102	2	Betrieb
		Hörsaal F107	1	Betrieb
	Fachsprachenzentrum	F-Trakt, SG	2	Betrieb
		H-Trakt, 1.OG, 2.OG	5	Betrieb
	Inst. f. Mathematik	EG	1	Betrieb
	Inst. f. Quantenoptik	1.-3.OG	3	Betrieb
	Unix-AG	1.OG	1	Betrieb
	Hochschulratsraum	1.OG, A105	1	Betrieb
1102	TIB/UB	Lesesäle	4	Betrieb
		Katalogsaal	1	Betrieb
		Gruppenarbeitsraum 2.OG	1	Betrieb
1103	Marstall	Lesesaal	1	Betrieb
1112	FB-Bibliothek Sozialwiss.	Leseraum EG, Empore	2	Betrieb
1146	FB-Bibliothek Geschichte/Religionswiss.	UG Lichthof, EG Katalogsaal	2	Betrieb
	Historisches Seminar	1.OG	3	Betrieb
		2.OG	1	Betrieb
1208	Weiterbildung Arbeitswiss.	EG-1.OG	3	Betrieb
1210A	RRZN	2.OG	5	Betrieb
		2.OG Bibliothek	1	Betrieb
		EG	3	Betrieb
		EG	2	Betrieb
		EG Ausbildungsraum	1	Betrieb
1210B	Weiterbildung Arbeitswiss.	UG, 2.OG, 4.OG	3	Betrieb

WLAN-Topografie

Gebäude	Bezeichnung	Geschoss	APs	Bemerkungen
11501	Conti Campus	Außenbereich	1	Betrieb
		EG R046, R063, R001	3	Betrieb
		1.OG R112, R171	2	Betrieb
		Hörsaal 201	2	Betrieb
		Hörsaal 301	2	Betrieb
		3.OG R332, R348	3	Betrieb
		4.OG R401, R442	4	Betrieb
1502	Hochhaus	8.OG	1	Betrieb
1502	Hochhaus	8.OG	1	Betrieb
1503	Conti Campus	Außenbereich	1	Betrieb
1504	Fachber.bibliothek Conti-Campus	EG-4.OG	25	Betrieb
1507		Hörsäle VII002, VII003	4	Betrieb
		Hörsaal 126	3	Betrieb
		EG Vorraum, R124	2	Betrieb
1801	Sportinstitut	EG, KG, Außenbereich	4	Betrieb
3109	Schneiderberg 50	2.OG	1	Betrieb
		EG	2	Betrieb
		3.OG	1	Betrieb
3110	Hauptmensa	EG	2	Betrieb
3401	Albert-Einstein-Institut	1.OG	2	Betrieb
3403	Mechanik/Regelungstechnik	R129, R139	3	Betrieb
		KG, Raum 250A	1	Betrieb
3405	Albert-Einstein-Institut	1.OG	2	Betrieb
3407	Inst. f. Bauinformatik		1	Betrieb
	Unix-AG	2.OG	1	Betrieb

WLAN-Topografie

Gebäude	Bezeichnung	Geschoss	APs	Bemerkungen
13408	Appelstr. 9a	EG	3	Betrieb
		Hörsaal MZ1	3	Betrieb
		Hörsaal MZ2	2	Betrieb
		Baumechanik (1.OG)	2	Betrieb
		Curt-Risch-Inst. (4.OG)	3	Betrieb
		Inst. f. Kartographie (6.OG)	3	Betrieb
		Inst. f. Verkehrswirtsch. (7.OG)	3	Betrieb
		GEML (10.OG)	2	Betrieb
		GEML (11.OG)	4	Betrieb
		GEML (12.OG)	2	Betrieb
		TNT (13.OG)	4	Betrieb
		ANT (14.OG)	4	Betrieb
		ANT (15.OG)	4	Betrieb
3702	LfI	EG, Hörsaal	3	Betrieb
3703	TI-Gebäude	EG, Eingangsbereich	1	Betrieb
		EG, Konferenzraum	1	Betrieb
		EG, Laborraum	2	Betrieb
		EG, Multimedia-Hörsaal	3	Betrieb
		1. OG	4	Betrieb
		2. OG	4	Betrieb
		4. OG	1	Betrieb
	Fachschaft Inf.	EG	1	Betrieb
4105	Herrenhäuser Str. 2	KG	1	Betrieb
		A-Trakt, EG	3	Betrieb
		C-Trakt, EG-2.OG	5	Betrieb
		D-Trakt, EG-2.OG	8	Betrieb
		F-Trakt, EG	2	Betrieb
		F-Trakt, 1.OG	2	Betrieb
		E/F-Trakt, 2.OG	3	Betrieb
		E111/Blaue Grotte	2	Betrieb
4107	Herrenhäuser Str. 2a	EG	2	Betrieb
		1.OG	2	Betrieb
		R009 Hörsaal	2	Betrieb

WLAN-Topografie

Gebäude	Bezeichnung	Geschoss	APs	Bemerkungen
14113	Biophysik	1.OG A101A, A118	2	Aufbau
		DG	2	Aufbau
4134		1.OG	1	Aufbau
4136		2.OG	1	Betrieb
4201	Herrenhäuser Str. 8	Foyer	3	Betrieb
		Ausstellung	2	Betrieb
		Hörsaal	2	Betrieb
6304	Bismarckstr.	EG, KG	5	Betrieb
6401	L3S	1.OG	2	Betrieb
8110	PZH	EG Spine	4	Betrieb
		EG Hörsaal	3	Betrieb
		EG	4	Betrieb
		1.OG	3	Betrieb
8111	PZH	1.OG	1	Aufbau
8113	PZH	3.OG Flur	3	Aufbau

Was wird benötigt?

- Funknetzkarte
  Ist in den meisten aktuellen Notebooks Standard
- Account auf dem Terminalserver
- Cisco-VPN-Klient für Linux
  `ftp.rrzn.uni-hannover.de/pub/local/vpn/linux`
- oder `vpnc`-Klient (OpenSource) für Linux
- Konfigurationsprofile für die Klienten
- Netzwerkname (ESSID): `UHWLAN`

Profile vpnc

Zugang aus dem WLAN (/etc/vpnc/wlan.conf):

```
IPSec gateway 192.168.10.3
IPSec ID wlanv
IPSec secret wlanv4mobil
Xauth username zzzzkurs
```

Zugang aus einem Festnetz (/etc/vpnc/internet.conf):

```
IPSec gateway 130.75.2.40
IPSec ID interv
IPSec secret interv4mobil
Xauth username zzzzkurs
```

Sicherheitsrisiken im Funknetz

- VPN ist nicht zwangsläufig aktiviert.
- Freigaben im selben Subnetz (192.168.10.x) sichtbar
- ohne VPN sind alle Netzwerkverbindungen (Freigaben etc.) im selben Subnetz unverschlüsselt.