Tübix 2017: Lightning Talk rdiff-backup

- Python Skript [last release version 1.2.8, 2009]

- Backup Planung:

  lokal (Wechseldatenträger), Intranet/Internet, GUI, Scripting, root/non-root, Daemon ja/nein, Client-Server-Struktur, zentral/dezentral, Synchronisation/Mirror/Snapshot, Transferrichtung, Verschlüsselung, plattformübergreifend, dateisystem(un)abhängig, Delta-Funktionalität, Hardlinks, extended attributes (xattr), ACL, SELinux, ..

- Beispielszenario: Große Datei, kleine Änderung

  - lokal
  - Netzwerk-Mount (pseudo-lokal)
  - Client-Server / Daemon

Backup Features (Auswahl):

- Minimalistisch, ausgereift, easy-to-use
- gute SSH-Integration
- sichert u.a. auch fifo-, socket-, symlink-, device-Files und Hardlinks.
- Unterstützung für ACL und xattr
  (Zus. Pakete nötig: pylibacl, pyxattr für ACL resp. xattr – keine automat. Installation)
- Extraverzeichnis [`rdiff-backup-data`] für Diffs und Metadaten (sonst nichts)
- Plattformunabhängig (dateisystemunabhängig), verfügbar für Linux, BSD, Windows, MacOS
- kein Daemon notwendig, Remote-Command via SSH (beidseitige CPU-Nutzung)
- Hohe Flexibilität bei Automation mittels Scripting

Backup konkret:

On localhost: `$ rdiff-backup /path/to/folder /mnt/backup`

To remote Host: `$ rdiff-backup /path/to/folder user@remotePC::/mnt/Backup`

Restore Features (Auswahl):

- Transparentes Backupformat (Mirror inkl. Snapshots)
- unabhängig von rdiff-backup möglich (reverse-deltas vs. forward deltas)
- FUSE verfügbar (rdiff-backup-fs), Snapshots als „normale Verzeichnisstruktur“ zugänglich

Restore konkret:

On localhost: `$ rdiff-backup -r now /mnt/backup /path/to/folder`

To remote Host: `$ rdiff-backup -r now user@remotePC::/mnt/Backup /path/to/folder`

Ausgangssituation: Regelmäßiges Backup eines Servers

- Trennung von System und Userdaten/Content:
  - System in KVM
  - Userdaten/Content per P9FS in KVM eingebunden
- Dateirechte auf Hypervisor (mapped accessmode):
  `drwxr----- 9 libvirt-qemu libvirt-qemu 4096 Jun 21 12:26 /mnt/Daten/`
- Dateirechte in der KVM werden in extended attributes (xattr) abgelegt
  (xattr anzeigen: `$ attr -l /path/to/file`)
- ein Backupdienst für alle (virtuellen) Systeme auf Hypervisor ausreichend, keine Einrichtung innerhalb jeder KVM notwendig
- Backupprozess soll nicht als root ausgeführt werden (müssen)
- Dateirechte (inkl. xattr) müssen beibehalten werden
  (Eigentümer wechselt jedoch wenn nicht als root ausgeführt)
- Datentransfer via Internet (Bandbreite, Trafficvolumen, Zeit)

Absicherung: Backupserver kompromittiert! Was nun?

- Unprivilegierter User-Account rbackup (mit stark eingeschränkten Rechten) erstellt.
- Minimalistische, ausgereifte Software (Python Skript) → geringer Angriffsvektor
- Kein Daemon, keine Client-Server-Struktur, kein (zus.) offener Port
- Verschlüsselung, Authentifizierung, Absicherung durch SSH (UNIX Philosophie)
- SSH Remote-Command Restriktionen:

```
# vi /home/rbackup/.ssh/authorized_keys
from="192.168.249.20",command="rdiff-backup --server --restrict-read-only /mnt/Daten",no-port-forwarding,no-X11-forwarding,no-pty ssh-rsa AAAAB3NzaC1yc2E...
```

Links:

- Projektseite: http://rdiff-backup.nongnu.org/
- Wikipedia: https://de.wikipedia.org/wiki/Rdiff-backup