Backup

Wieso, weshalb, warum?

Warum?

- Doppelter Boden, falls mal was passiert…
- 90% der Fälle: Ich habe eine Datei gelöscht und brauche die DRINGEND wieder!
- Was sind mir meine Daten wert?
- Was kostet es mich meine Daten wieder herzustellen (aus den ursprünglichen Quellen - wenn vorhanden)?

Was?

- Welche Daten kann ich nicht mit geringem bzw. geringsten Aufwand wieder herstellen?
- Welche Daten habe ich / haben wir selbst erzeugt?
- Mit welchen Daten verdiene ich mein Geld?
- Was ist für mich Wertvoll (Erinnerungsphotos, …)?

Wie?

- Einfaches Kopieren auf Festplatten,
- auf einen Server mit rsnapshot auf Festplatten sichern,
- auf einen anderen Server mit bareos auf Festplatten und / oder Tape sichern.

Festplatten

- Immer eine Vollsicherung?
  - … u.U. braucht man dafür viele Festplatten,
  - … kann teuer werden.
- Für diff. und inkr. Sicherungen braucht man Software:
  - TimeMachine (MacOS),
  - Acronis (Win).

rsnapshot #1

- Wrapper für rsync,
- kann gut auf Festplatten sichern,
- Daten liegen auf einem anderen Server inkl. Historie,
- auf die Daten kann direkt zugegriffen werden.

bareos #1

- bacula Fork,
- kann auf Festplatten sichern,
- kann auf Tapes sichern,
- kann auch auf Tapelibraries sichern,
- kann Sicherungen verschlüsseln,
- stellt Historie zur Verfügung.

Backup unter Sicherheitsaspekten betrachtet

- Drei Säulen der IT-Sicherheit:
  - Vertraulichkeit,
  - Integrität,
  - Verfügbarkeit.

Vertraulichkeit

- Ich muss sicherstellen das meine Daten auf dem Transportweg und auf den Zielmedien NICHT manipuliert werden können.
- Da hilft uns Crypto. ;-)

Integrität

- Ich muss sicherstellen, dass die Daten vom Client auch unverändert und VOLLSTÄNDIG auf das Sicherungsmedium geschrieben werden.
- Hierfür gibts Checksum und Crypto.

Verfügbarkeit

- Rücksicherung in akzeptablen Zeiten.
- Die Wiederherstellung der gesicherten Daten muss mind. einmal in der Woche auf Korrektheit überprüft werden.
  - BACKUP MUSS GELEBT WERDEN!!!

Die Anforderungen

- Transportverschlüsselung,
- Verifizierung der übertragenen Daten,
- Medienverschlüsselung,
- bei Festplattensicherung: RAID1 oder RAID5 oder RAID6,
- sicheren Aufbewahrungsort für Bänder,
- OnTop:
  - Desasterrecovery für komplette Rechner,
  - Benachrichtigung via E-Mail, Jabber, etc.

rsnapshot #2

- rsync-Wrapper,
- Transportverschlüsselung via SSH (Übertragungsgeschwindigkeit!),
- Backupmedien (Festplatten) müssen mit OS-Boardmitteln verschlüsselt werden,
- wird über cron aufgerufen,
- Konfiguration über eine einzige Datei (… achtet auf die Tabulatoren).

rsnapshot #3

- Die Daten liegen auf den Festplatten
  - … und sind zeitlich versioniert.
  - Die Daten können durch einfaches Kopieren aus den Verzeichnissen zu den verschiedene Zeitpunkten wieder hergestellt werden.

rsnapshot #4

- Historie:
  - stündliche Sicherungen (z.B. alle zwei Stunden),
  - tägliche Sicherung (wird i.d.R. sieben Tage vorgehalten),
  - Wochensicherung (wird i.d.R. vier Wochen vorgehalten),
  - Monatssicherung (wird i.d.R. drei Monate vorgehalten).
- Hardlinks im Dateisystem

rsnapshot #5

- Wie geht das mit der Versionierung?
  - Aus der ältesten Stundensicherung wird die erste Tagessicherung (tägliche Aktion),
  - aus der ältesten Tagessicherung wird die erste Wochensicherung (wöchentliche Aktion),
  - aus der ältesten Wochensicherung wird die erste Monatssicherung (monatliche Aktion),
  - nach drei Monaten wird die älteste Monatssicherung verworfen.

bareos #2

- Dreiteiliger Aufbau,
- kann mit verschiedene Sicherungsmedien umgehen,
- Transportverschlüsselung via TLS,
- Medienverschlüsselung via Software,
- bei Tapes (LTO) auch Hardwareverschlüsselung,
- Zugriff mehrere Backupoperatoren:
  - Berechtigungen werden über ACLs eingestellt.

bareos #3

- Aufbau:
  - Director - die Steuerzentrale,
  - Storage Daemon - schreibt die Backupdaten auf die Medien und steuert ggf. Tapelibs,
  - File Daemon - das ist der Client der die Daten von den zu sichernden Rechnern einsammelt.

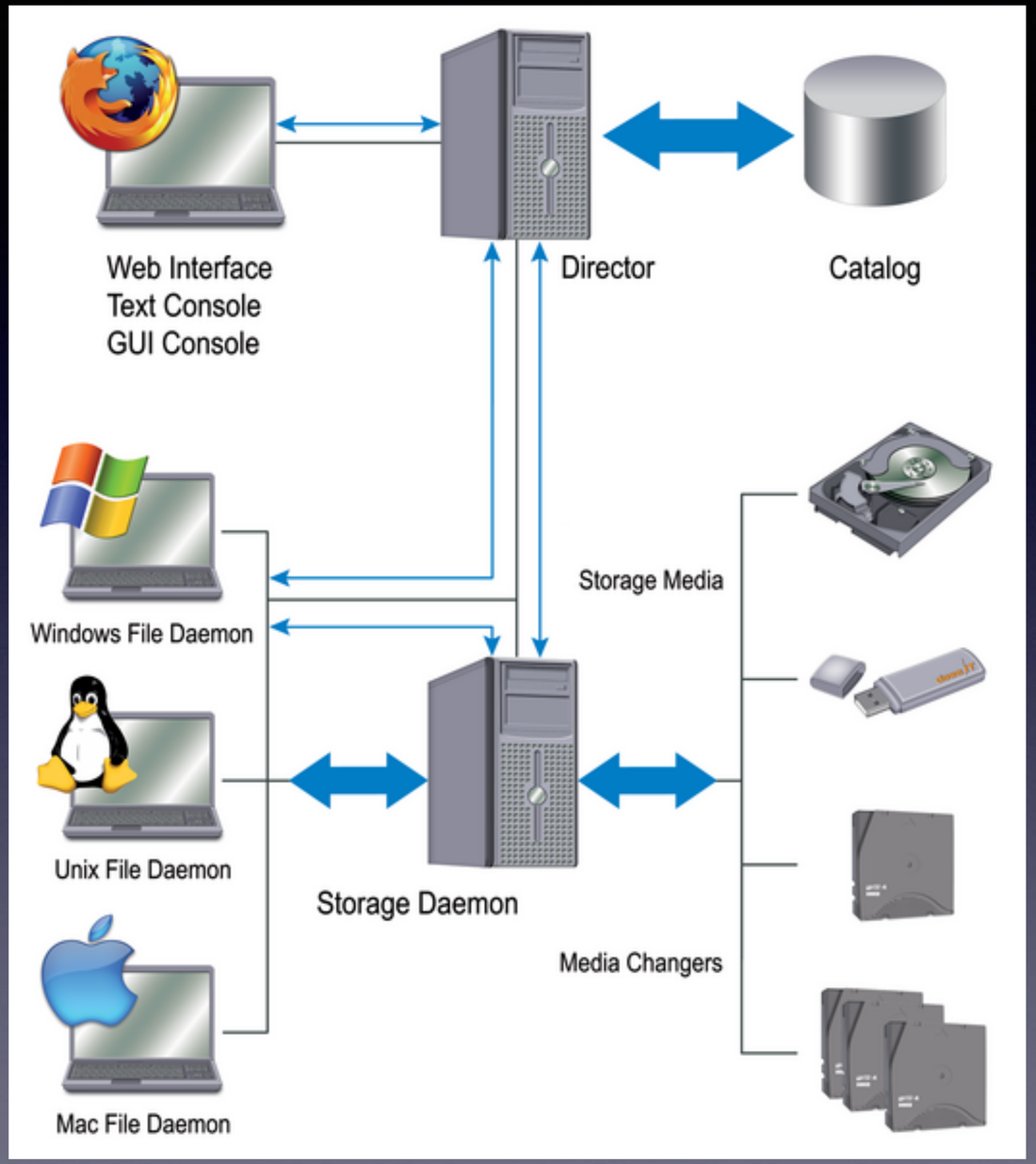
bareos #4

- Durch die Teilung der einzelnen Komponenten kann bareos verteilt installiert werden

bareos #5

Mögliches Szenario

Bildquelle: http://www.admin-magazin.de/Das-Heft/2013/05/Neue-Features-im-Bacula-Fork-Bareos



bareos #6

- Backuptypen (Full, Diff, Inc) werden i.d.R. auf verschiedene Pools verteilt,
- Pools enthalten Medien (Bänder oder Volume-Dateien),
- Volumes, Backups werden mit „Verfallsdatum“ konfiguriert.

bareos #7

- Die versch. Backuptypen können auch auf versch. Speichermedien verteilt werden, z.B.:
  - Full auf LTO,
  - Diff und Inc auf Festplatte.
- Mit „Migration-Jobs“ können Backups auch auf andere Medien übertragen werden,
- Backup2Disk2Tape.

baroes #8

- Konfigurationsbestandteile
  - Storage -> Auf welches Medium soll gespeichert werden?
  - Pool -> Fasst Volumes zusammen.
  - Client -> Welche Rechnern sollen gesichert werden?
  - FileSet -> Welche Dateien sollen gesichert werden?
  - Schedule -> Zu welchen Zeiten soll gesichert werden?
  - Job -> Was soll wann, wie auf welches Medium geschert werden?

bareos #9

- Warum bareos und nicht bacula?
  - Die „fency features“ kosten bei bacula Geld,
    - Grund für fork.
  - Rechtliche Auseinandersetzung zwischen Kern Siebald (bacula Erfinder) und den bareos Jungs.
    - Stand???

bareos #10

- Zum weiterlesen:
  - http://www.admin-magazin.de/Das-Heft/2013/05/Neue-Features-im-Bacula-Fork-Bareos
  - http://www.admin-magazin.de/Das-Heft/2015/06/Workshop-Aufbau-und-Inbetriebnahme-von-Bareos
  - Philipp Sturz: Bacula
    - ISBN der Print-Ausgabe: 978-3-941841-41-3
    - ISBN (E-Book, PDF) 978-3-941841-83-3

Backup muss gelebt werden

…am besten täglich