

MODUL 143

BACKUP- U. RESTORE- SYSTEME IMPLEMENTIEREN

Gerhard.Beutler

Sicherung 1: Vollsicherung einer Webseite

Lernziele

- Vollsicherung beschreiben, unterscheiden und erkennen.
- Problematik der Dateiattribute kennen und verstehen.
- Vollsicherung praktisch umsetzen.
- Shell-Befehle für Vollsicherung anwenden.

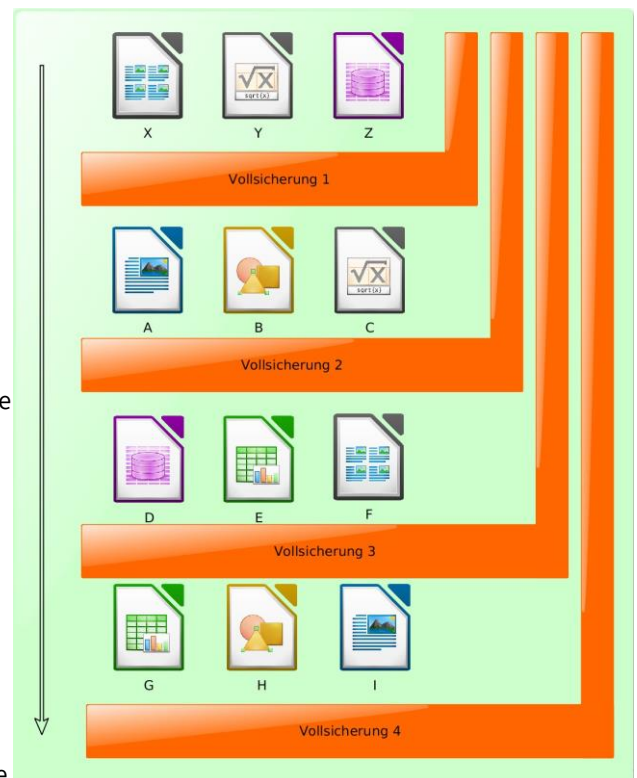
1.1 Theorie: Vollsicherung

Vollsicherungen zeichnen sich dadurch aus, dass sie einen Datenbestand komplett abbilden. In einfachen Worten: eine Kopie der gesamten Daten. Eine Vollsicherung repräsentiert somit genau jenen Zu- stand, als die Sicherung gemacht wurde.

Da bei jedem Mal erneut alle Daten gesichert wer- den, werden mehrere Vollsicherungen über längere Zeit verhältnismässig gross. Dies kann ein Problem hinsichtlich Leistung und Speicherbedarf darstellen! Vollsicherungen nehmen viel Zeit und Systemressourcen in Anspruch, was als Nachteil betrachtet werden kann. Der Vorteil ist, das alle Daten beieinander sind und eine Wiederherstellung des Systems vergleichsweise einfach ist.

Die folgende Grafik stellt den Ablauf einer Vollsicherung schematisch dar. Es finden vier Vollsicherungen (V1-V4) statt. Dazwischen geschehen Änderungen (A- I) an den Daten (X,Y,Z).

Der Einfachheit wegen wird angenommen, dass nur neue Dateien hinzukommen. Es wird aber nichts gelöscht und existierende Dateien werden nicht verändert. Markieren Sie (z.B. mit einem Kreuz), welche Daten in welchem Fullbackup enthalten sind:



	X	Y	Z	A	B	C	D	E	F	G	H	I
V1												
V2												
V3												
V4												

Wenn Sie also Beispielsweise Ihren persönlichen Ordner komplett auf einen USB-Stick ziehen, dann ist das bereits eine Vollsicherung! In einem professionellen Umfeld gibt es aber noch einige Dinge zusätzlich zu be- achten:



Aufgabe 1)

Begründen Sie selbstständig oder mit Ihrem Sitznachbarn, warum diese beiden Punkte bei Sicherungen wichtig sind.

- Der **Zugriff** auf die Sicherung muss genau so geschützt/kontrolliert sein wie die Originaldaten.
Begründung:

-

.....

.....

.....

- Die **Dateiattribute** jeder einzelnen Datei müssen beim Kopiervorgang erhalten bleiben.
Begründung:

.....

.....

.....

1.3 Vorbereitung: Linux-Kommandos zur Vollsicherung



Wir steigen wieder ins Fallbeispiel aus der ersten Lektion ein. Sorgen Sie dafür, dass Ihre Webseite läuft und Sie vom Desktop her darauf Zugriff haben. Erst wenn Sie soweit sind, kann mit dem Arbeitsblatt fortgefahren werden.

In der Praxis gibt es viele verschiedene Möglichkeiten eine Vollsicherung durchzuführen. Die Art der Umsetzung hängt von der Firma, der technischen Umgebung und der Art der zu sichernden Daten ab. Es gibt frei verfügbare und kommerzielle Software-Produkte, die sich jeweils in der Bedienung unterscheiden. Es ist daher wichtig neben einem spezifischen «Tool» auch die Konzepte zu verstehen, welche dabei zur Anwendung kommen. Die Anwendung einer bestimmten Software muss dann von Fall zu Fall erlernt werden. Für Vollsicherungen genügt im Prinzip die Basis-Software, welche mit jedem Betriebssystem mitgeliefert wird: Programme zum Kopieren von Dateien. Unter Linux steht uns hier eine grosse «Werkzeugkiste» zur Verfügung. Schauen wir uns einige der einfacheren Möglichkeiten an:

- `cp` - Kopiert eine Datei oder eine Verzeichnisstruktur.
- `scp` - Kopiert eine Datei oder eine Verzeichnisstruktur verschlüsselt über ein Netzwerk.
- `tar` - Erstellt ein Archiv einer Verzeichnisstruktur.
- `zip` - Erstellt ein Archiv einer Verzeichnisstruktur.



Sie müssen `zip` erst installieren, damit Sie damit arbeiten können:



vmadmin@vmLS3: ~\$

```
sudo apt install zip
```



Notiz

Erstellen Sie eine Übersicht über die Kommandos zum Sichern und wie dabei die Dateiattribute bewahrt werden können. Die folgenden Optionen sind wichtig und sollten beschrieben werden:

- `cp` : `-a`, `(-d, -R, -p, --preserve=all)`
- `scp`: `-r`, `-p`
- `tar`: `-c`, `-x`, `-z`, `-v`, `-f`
- `zip`: `-r`, `-y`

Nutzen Sie Man-Pages, die Option `--help` oder das Internet zur Informationsbeschaffung. Ausprobieren erlaubt und erwünscht!

.....

.....

Aufgabe 2

Versuchen Sie anhand der Parameter zu beschreiben, was die jeweiligen Kommandos machen. Experimentieren Sie bei Bedarf mit den Kommandos auf der Konsole!

Achtung: Die Kommandos funktionieren meist nicht 1:1 auf dem Server. Sie müssten die Beispieldateien erstellen, wenn Sie es genau so ausführen möchten.

- `cp -a /home/vmadmin /media/vmadmin/USBbackup`

Erklärung:

.....

.....

- `scp backup_2015-08-01.zip vmadmin@192.168.240.65: /backups`

Erklärung:

.....

.....

- `tar czvf /tmp/vmadmin.tgz /home/vmadmin`

Erklärung:

.....

.....

- `tar xzvf vmadmin.tgz`

Erklärung:

.....

.....

- `zip -r config.zip /etc`

Erklärung:

.....

.....

- `unzip config.zip`

Erklärung:

.....

1.4 Umsetzung: Vollsicherung der Webseite

Wir wollen nun mit Hilfe einiger der eben kennengelernten Tools ein Backup der Daten auf dem Applikations-server erstellen. Wir haben im Moment die folgenden Daten zu sichern:

- ›Die Datei logo.jpg, entweder in Ihrer eigenen Version oder unter /usr/share/loroweb/.
- Die Datei hallo.txt, entweder in Ihrer eigenen Version oder unter /etc/loroweb.conf.



Aufgabe 3)

Bereiten Sie für den Applikationsserver die zu sichernden Daten vor.

1. Entscheiden Sie sich welches logo.jpg sie sichern wollen. Absoluter Pfad zur Datei:

.....

2. Entscheiden Sie sich welches hallo.txt sie sichern wollen. Absoluter Pfad zur Datei:

.....

3. Machen Sie eine temporäre lokale Sicherheitskopie Ihrer Daten mit cp -a nach /tmp. Damit stellen wir sicher, dass nichts verloren geht, falls beim jetzt folgenden Erstellen eines Archives etwas schief geht! Befehl:

.....

4. Packen Sie Ihre originalen Dateien in ein komprimiertes Archiv mittels tar oder zip. Befehl:

.....

5. Kopieren Sie das Archiv (vom Backup-Server her eingeloggt) mittels scp vom Applikationsserver zu Ihnen auf den Backupserver, in ein zu erstellendes Verzeichnis

/home/vmadmin/m143/ab03. Befehl:

.....

6. Kontrollieren Sie mit ls -l ob die Sicherung auf dem Backupserver angekommen ist und eine relevante Dateigrösse besitzt (grösser als 0 Byte!). Ausserdem können Sie sich mit

tar -tf oder unzip -l den Inhalt des Archivs anzeigen lassen. Prüfen Sie also zur Sicherheit auch ob die Dateien im Archiv gelistet sind.

Gratulation: Sie haben ein erstes Fullbackup auf einer Serverumgebung durchgeführt!





Aufgabe 4)

Machen Sie ein zweites Fullbackup. Nutzen Sie jetzt aber ausschliesslich das Kommando scp mit den Optionen

-r und -p!

Damit etwas mehr Daten (als im Moment das Fallbeispiel hergibt) zur Verfügung stehen, nutzen wir Pseudo-Daten. Installieren Sie sich das Paket m143-03-randomfiles auf dem Applikationsserver. Führen Sie es danach z.B. in /m143/ab03 aus (randomfiles aufrufen). Es sollten zufällige Dateien in einem Ordner data generiert worden sein!

Einen guten Überblick über die Dateien liefert Ihnen das Kommando tree (muss evtl. über apt nachinstalliert werden) oder auch ein kombiniertes find-Kommando wie z.B:

```
find data
```

```
find data -type f
```

```
find data -type f -exec ls -l {} \;
```

Sichern Sie nun diesen Ordner mit Zufallsdaten auf den Backupserver! Prüfen Sie am Schluss sporadisch ob die Dateirechte auf beiden Maschinen gleich geblieben sind.

.....

.....

1.5 Abschluss

Reflexion



Mit welchen Hilfsmitteln können Sie einfache Vollsicherungen durchführen? Was für Optionen haben Sie tatsächlich benutzt? In welchen unterschiedlichen Situationen braucht man cp, scp und wann tar oder zip? Wann könnten tree und find nützlich sein?

.....

.....

.....

.....

.....



2. Sicherung 1: Wiederherstellung Vollsicherung

Lernziele

- Einfaches Datensicherheitskonzept für eine Vollsicherung erstellen.
- Speicherlauf und Anforderung einer Vollsicherung abschätzen.
- Vor- und Nachteile einer Vollsicherung benennen.
- Wiederherstellung einer Vollsicherung umsetzen.

2.1 Datensicherheitskonzept



Wir haben die Vollsicherung bis jetzt einfach «blind» durchgeführt. Im Vordergrund standen technische Schwierigkeiten. Bei produktiv relevanten Sicherungen müssen aber erst einige organisatorische Abklärungen vorgenommen werden! Erst dies erlaubt es mittels Datensicherheitskonzept eine vollwertige Sicherung anzulegen.

2.1.1 Anforderungen Fallbeispiel

Wegen des fehlenden Datensicherheitskonzeptes planen Sie eine Sitzung mit Ihrem Chef. Er selbst versteht von Informatik nicht viel (dafür sind Sie der Experte). Anbei Ihre Notizen aus dem Gespräch:

- Zu sichern sind Begrüssungs-Text und Logo.
- Das Logo verändert sich evtl. 1x pro Jahr. Der Text kann etwa jede Woche wechseln.
- Es soll eine Vollsicherung gemacht werden.
- Die Sicherung soll immer am Donnerstag Abend manuell ausgeführt werden.
- Eine Anleitung für Backup und Restore ist zu erstellen.



Aufgabe 1)

Erstellen Sie nun aufgrund der Sitzung sowie den Informationen, welche Sie durch die erste Vollsicherung haben, ein Datensicherheitskonzept mit einem Jahr Gültigkeit. Sie können hierfür die Vorlage auf der nächsten Seite verwenden.

Tauschen Sie sich bei kleineren Problemen gegebenenfalls mit dem Sitznachbarn oder in der Gruppe aus!

2.1.2 Vorlage Datensicherheitskonzept Webserver

Zu sichernde Daten

Pfad	Grösse	Delta/Woche	Vorarbeit

Sicherungsverfahren

Sicherungsverfahren	
Aufbewahrungsort	
Namensschema Datei	
Kommandos Durchführung	
Zeitpunkt Durchführung	

Wiederherstellung

Vorbereitende Arbeiten	
Wiederherstellung	
Abschliessende Arbeiten	

Verantwortlichkeit

Name:		Ort:	
Unterschrift:		Datum:	

2.2 Wiederherstellung



Aufgabe 2)

Korumpieren Sie nochmals die Daten auf Ihrem Applikationsserver. (z.B. auf dem Server mit `rm` oder vom Büro-PC her mit `boes`).



Aufgabe 3)

Stellen Sie die «kaputten» Daten des Applikationsservers wieder her. Verwenden Sie dazu Ihr vorher erstelltes Datensicherheitskonzept. Falls Sie Probleme bei der Wiederherstellung haben, verbessern oder ergänzen Sie das Datensicherheitskonzept entsprechend. Gibt es in diesem Fall Unterschiede zwischen Backup- und Restore-Kommandos? Notieren Sie die Kommandos für Backup und Restore in Ihrem Notizbuch.

.....

.....



2.3 Abschätzung Speicherplatz

Beim vorhin erstellten Datensicherheitskonzept wurde ein wichtiger Aspekt weggelassen: Wichtig für ein Datensicherheitskonzept ist die Vorausplanung des Bedarfs an Speicherplatz! Wie lange wird man Backups auf den Datenträger speichern können, ohne das er «voll» ist? Um diese Frage geht es in diesem Kapitel.



Notiz

Die Grösse einer Datei können Sie sich mit `ls -lh`, die Grösse eines Ordners mit `du -sh` anzeigen lassen. Den freien Platz auf einer Partition können Sie mit `df -h` herausfinden.



Aufgabe 4)

In unserem Fallbeispiel ist das Berechnen des verbrauchten Speicherplatzes relativ einfach, *denn die Daten bleiben immer etwa gleich gross*. Auch wenn wir den Text etwas anpassen oder die Grafik verschönern, die Grösse der Daten verändert sich kaum. Wie gross ist das Backup aus dem Fallbeispiel?

.....

.....

.....

Anders ist es, wenn die Daten ständig anwachsen. Das Berechnen des benötigten Speicherplatzes für mehrere Vollsicherungen wird dann anspruchsvoller. Wenn man eine konstante, gleichbleibende (d.h. lineare) Zunahme annimmt, lautet die korrekte Formel hierfür:



$$y = (x + 0.5 \cdot t \cdot d)(1 + t)$$

Wenn gilt:

- y ist der insgesamt belegte Speicherplatz aller Vollsicherungen
- x ist die Grösse des allerersten, initialen Vollbackups, z.B. 5GB.
- d ist das konstante Delta, also die geschätzte Grösse an Daten, welche zwischen den Backups hinzukommt. Beispielsweise 0.5GB.
- t ist die Zeit, d.h. wie oft eine Vollsicherung gemacht wird. Ein Jahr lang tägliches Sichern gäbe z.B. $t = 364$. Achtung die allererste Sicherung ist $t = 0$.



Aufgabe 5)

Wie hoch wäre der insgesamt beanspruchte Speicherplatz mit den obigen Beispielswerten? Also: erste Sicherung mit 5GB

an Daten, tägliches Backup ein Jahr lang. Jeden Tag kommen etwa 0.5GB hinzu?

.....

.....

.....

.....

Ist an dem Resultat etwas überraschend? Ziehen Sie ein Fazit und erklären Sie das Ergebnis:

.....

.....

.....

.....

.....

.....

.....

2.4 Repetition & Abschluss



Aufgabe 6)

- Nennen Sie 4 **zentrale** Bestandteile eines Datensicherheitskonzepts

.....

.....

- Nennen Sie je ein Vor- und Nachteil der Vollsicherung.

.....

.....

.....

.....

- Was bewirkt die Option -y beim Programm zip? Was geschieht wenn man die Option nicht auswählt? Wie ist es mit tar?

.....

.....

.....

- Mit welchem Kommando kopieren Sie die lokale Datei back.zip auf den Server backup.schule.bsp in das Ver- zeichnis /home/files? Der Benutzer des Servers heisst files.

.....

- Mit welchem Kommando kopieren Sie das Verzeichnis /data nach /backup/data, ohne die Dateirechte zu ver- ändern?

.....

- Mit welchem Kommando packen Sie das Verzeichnis ~/data in ein Archiv
~/data_2015-09-23.tgz?

.....



Aufgabe 7)

- ›Das Kommando `du -sh` gibt die belegte Grösse des zusichernden Heimverzeichnisses mit 11G an. Auf dem Backupserver zeigt `df -h` unter Verfügbar 950G an. Jede Woche kommen 1G an Daten hinzu. Es wird wöchentlich eine Vollsicherung gemacht.

Reicht der Backupserver für ein Jahr? (Berechnung hinschreiben)

.....

.....

.....

Reicht der Platz, wenn stattdessen nur alle zwei Wochen gesichert wird?

.....

.....

.....



Reflexion

Fassen Sie zusammen: Was für Bedingungen braucht es für ein erfolgreiches Restore?

.....

.....

.....

.....

.....

.....

.....

.....

