smartlearn
virtual learning. real success.

MODUL 143

BACKUP- U. RESTORE-SYSTEME IMPLEMENTIEREN

Gerhard.Beutler

1 Wechselschemas

Lernziele

- Die drei Wechselalgorithmen beschreiben und erkennen.
- Aufbewahrungsdauer für die drei Wechselschemas berechnen.

1.1 Was ist ein Wechselschema?

Wenn Sie Daten Sichern, brauchen Sie immer irgendeine Art von Speichermedium:

Damit ist es aber meist nicht getan. In der Praxis ändern sich die Originaldaten laufend, d.h. es müssen immer wieder neue Sicherungen gemacht werden. Irgendwann stossen Sie an die Grenzen der Speicherkapazität des verwendeten Mediums.

Wir haben Strategien kennengelernt, welche das Problem der stetig anwachsenden Datenberge etwas entschärfen: differenzielle oder inkrementelle Sicherungen als Ergänzung zur Vollsicherung. Doch auch diese Verfahren lösen das Problem nicht:

Irgendwann kommen Sie immer in die Situation, dass Sie das Sicherungsmedium wechseln müssen um Datenverlust zu vermeiden!

Im Prinzip lässt sich immer ein neues Medium verwenden, wenn das alte Medium beschriftet zur Seite gelegt wird. Dieser Prozess lässt sich aber nicht andauernd weiterführen. Irgendwann ist der «Backup-Tresor» überfüllt, oder das Budget für neue Speichermedien ist aufgebraucht.

Um diesen «Teufelskreis» von stetem Wachstum zu durchbrechen, werden Wechselschemas verwendet: d.h. man bestimmt Regeln in welcher Art und Weise die Medien gewechselt werden. Hierzu werden zwei Entscheidungen benötigt:

1. Wie viele Speichermedien sollen verwendet werden? Es wird eine fixe Anzahl festgelegt! Beispiel: Es werden genau sieben USB-Sticks verwendet.
2. Nach welchem Schema werden die Speichermedien ausgewechselt? Wann werden die alten Daten eines Mediums mit neuen Daten überschrieben? Beispiel: Immer am Montag wird der Tages-USB-Stick vom letzten Montag mit den neuen Daten überschrieben.

Sie merken: **Wechselschemas führen zum Verlust alter Backup-Daten**! Es wird aber versucht diesen «Verlust» durch einen geschickt gewählten Algorithmus möglichst geschickt zu steuern, bzw. zu «managen». Getreu dem Motto:

Lieber kontrollierter Verlust als ewiges Wachstum.

1.2 FIFO

FIFO ist die Abkürzung für «First In, First Out», was auf Deutsch sinngemäss mit «Wer zuerst kommt, mahlt zuerst» übersetzt werden kann. Es handelt sich um die einfachste Variante einer Warteschlange, wie man sie an jeder Kasse kennt: Alle stellen sich hintereinander an und wer zuerst war, kommt zuerst dran.

Im Falle des Backups kann man sich das Szenario so vorstellen: Alle Speichermedien stellen sich hintereinander an. Bei jeder Sicherung kommt das «vorderste» Medium zum Einsatz. Ein genutztes Medium stellt sich wieder neu hinten an. Es wird also erst wieder überschrieben, wenn zuerst alle anderen Medien genutzt wurden.

Aufgabe 1)

In der obigen Abbildung werden 4 USB-Sticks verwendet. Wenn nun wöchentlich eine Vollsicherung durchgeführt wird, bis wie weit zurück können Daten «mit Garantie» wiederhergestellt werden? Schreiben Sie auch die Begründung!

.....

.....

.....

1.3Grossvater-Vater-Sohn

Unter «Grossvater-Vater-Sohn» versteht man eine etwas ausgeklügeltere und konkretisierte Variante des vorherigen FIFO- Prinzips. Um die zeitliche «Reichweite» der wiederherstellbaren Daten zu verlängern, werden drei FIFOs eingesetzt:

1. Sohn (1. FIFO): Tägliche Sicherung. Beispielsweise 4 Medien für Montag bis Donnerstag.
2. Vater (2. FIFO): Wöchentliche Sicherung. Beispielsweise 4 Medien für jede Woche im Monat.
3. Grossvater (3. FIFO): Monatliche Sicherung. Beispielsweise 12 Medien im Jahr.

Auf diese Weise entstehen zwar Lücken in der Sicherung (es lässt sich z.B. nicht jeder Tag von vor 4 Monaten wiederherstellen), dafür streckt sich aber die Zeit in welche die Backups hineinreichen beträchtlich. In diesem Beispiel wird mit nur 20 Speichermedien ein komplettes Jahr abgedeckt! Bei einer einfachen FIFO und täglicher Sicherung würde dies nur gerade für 20 Tage reichen, nun sind aber 365 Tage abgedeckt.

Aufgabe 2)

Erstellen Sie einen Monatsplan bis zum 31. des Monats. Gesichert werden soll nur an Arbeitstagen (Mo-Fr). Alle Sicherungen geschehen als Vollsicherung. Backups sollen maximal ein Monat

.....

Montag	Dienstag	Mittwoch	Donnerstag	Freitag	Sa.	So.
		1	2	3	4	5
6	7	8	9	10	11	12
13	…					

1.4 Türme von Hanoi

Der Algorithmus dieses Wechelschemas entspricht einem Knobelspiel namens «Türme von Hanoi». Der Name ist daher von diesem Spiel geborgt.

Aufgabe 3)

Falls Sie kein Holzspiel «Türme von Hanoi» zur Verfügung haben, gibt es auch Online-Varianten:

https://www.mathematik.ch/spiele/hanoi_mit_grafik/ (28.04.2016)

Lösen Sie das Spiel einmal mit drei Scheiben, und dann noch mit vier oder mehr. Was stellen Sie fest betreffend Züge welche gemacht werden müssen?

.....

.....

Auf eine tägliche Datensicherung angewendet, wird bei drei Medien wie folgt vorgegangen:

- Jedes Medium muss eindeutig und hierarchisch beschriftet werden. Beispiel: «A, B, C, …».
- Medium «A» wird jeden 2. Tag verwendet (Tag 1, 3, 5, . . .).
- Medium «B» wird jeden 4. Tag verwendet (Tag 2, 6, . . .).
- Medium «C» wird jeden 8. Tag verwendet (Tag 4, 8, . . .).

Dieses Vorgehen entspricht folgendermassen dem Spiel: Jede Scheibe des Spiels entspricht einem Speichermedium. Jedes Mal wenn eine Scheibe (korrekt) bewegt wird, heisst dies, dass eine Sicherung auf dieses Medium gespielt wird.

Es muss nicht zwingend täglich gesichert werden. Der «Wechselzyklus» ist frei wählbar. Es kann auch wöchentlich, monatlich oder «jeden 3. Tag im Jahr» gesichert werden.

Aufgabe 4)

Wann kommt welches Sicherungsmedium zum Einsatz, wenn 4 davon verwendet werden (Disk A, B, C und D)? Für einen optimalen Start werden zuerst alle Disks ein Mal initialisiert. Der Algorithmus startet erst *nach* «Wechsel 0». Füllen Sie die untenstehende Tabelle aus.

Wechsel:	*3*	*2*	*1*	*0*	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Disk A:	*i*				X														
Disk B:		*i*				X													
Disk C:			*i*																
Disk D:				*i*															

Das anfängliche Initialisieren aller Datenträger ist nicht Teil des Algorithmus. Es hilft aber die Backupverteilung beim Start des Ablaufs zu optimieren. Nach Ablauf des Algorythmus (Wechsel 15) wird wieder mit «Wechsel 1» begonnen.

1.4.1 Berechnung

Was ist nun der Vorteil des Wechselschemas «Türme von Hanoi»? Wie viele Speichermedien werden verwendet und bis wie lange reichen die Backups zurück? Um diese Fragen zu beantworten reicht eine einfache Formel:

$t = 2^n - 1$	Anzahl Züge des Spiels «Türme von Hanoi»
$t = 2^{n-1}$	Dauer bis das initiale/älteste Backup überschrieben wird
$t = 2^{n-2}$	jederzeit garantiertes Alter des ältesten Backups

Wenn gilt:

- t Ergebnis in Anzahl Wechselzyklen.
- n ist die Anzahl eingesetzter Medien.

Aufgabe 5)

Prüfen Sie die Formel auf das obige Tabellenbeispiel mit vier Speichermedien.

.....

Aufgabe 6)

Mit dem Schema «Grossvater-Vater-Sohn» führten 20 Medien zu einem Backup über die Dauer von einem Jahr, bei (ungefähr) täglicher Sicherung. Wenn Sie nun das Schema «Türme von Hanoi» verwenden, täglich sichern und 20 Medien zur Verfügung haben, wie lange geht es bis das letzte Medium überschrieben wird (und somit das älteste Backup verloren geht)?

.....

.....

Aufgabe 7)

Nennen Sie je mindestens einen Vor- und Nachteil des Wechselschemas «Türme von Hanoi».

.....

.....

1.5 Mischaufgaben

Aufgabe 8)

Füllen Sie die untenstehende Tabelle für alle Schemas aus. Es stehen 12 Speichermedien zur Verfügung, welche komplettes Fullbackup aufnehmen können. Gesichert werden soll täglich, inkl. Wochenende!

.....

.....

.....

.....

Schema	Medien	Zyklus	Tage bis ältester Restore
FIFO	12	täglich (Mo-So)	
Grossvater-Vater-Sohn	12	täglich (Mo-So)	
Türme von Hanoi	12	täglich (Mo-So)	

Aufgabe 9)

Können Wechselschemas auch auf Netzwerkspeicher bzw. auf die «Cloud» angewendet werden? Oder funktioniert dies nur mit greifbarer Hardware wie «Sticks» und «Disks»? (Nehmen Sie nur die Kundensicht. Wie die Daten gespeichert werden ist nicht relevant.) Begründen Sie:

.....

.....

.....

2 Sicherung 4: Systemsicherung

Lernziele

› Funktion und Nutzen eines Systemabbilds beschreiben.

› Live-System im VM-Player booten können.

2.1 System-Abbild

Wenn ein komplettes Betriebssystem mitsamt allen zusätzlich installierten und konfigurierten Programmen sowie allen Dateien gesichert werden soll, gibt es grundsätzlich zwei Möglichkeiten:

1. Hotbackup: Das Betriebssystem wird gesichert während es läuft. Hierzu sollten so wenige Anwendungen wie mög- lich laufen. Des Weiteren müssen Betriebssystem-spezifische Besonderheiten beachtet werden.
2. Coldbackup: Das Betriebssystem ist heruntergefahren. Das System wird von «aussen» (z.B. mittels Live-System) gesichert. Da das Betriebssystem selbst nicht läuft, können beim Sichern weniger Probleme auftreten. Dabei gibt es zwei Möglichkeiten:

   a) Sämtliche Dateien des Filesystems kopieren, oder

   b) ein komplettes Abbild (Englisch: Image) der Festplatte erzeugen.

Die verschiedenen Vorgehensweisen haben ihre eigenen Vor- und Nachteile.

Variante	Vorteil	Nachteil
1)	System muss nicht heruntergefah-ren werden.	Besonderheiten von Betriebssystemen und Applikationen müssen beachtet werden (mittels Fachwissen oder Spezialsoftware). Laufende Programme mit offenen Dateien können beim Kopiervorgang Inkonsistenzen verursachen.
2.a)	Inkrementelles sichern möglich. Dateien können einzeln wieder hergestellt werden.	Eigenheiten der Partitionen werden nicht gesi-chert. Dateisystem muss unterstützt werden.
2.b)	Einfaches und vom Betriebssys-tem unabhängiges Grundprinzip.	Einzelne Dateien können nicht oder nur mühsam wiederhergestellt werden. Braucht in der Re-gel viel Speicherplatz. Generell nur Fullbackups möglich.

In diesem Arbeitsblatt wollen wir uns auf das Erzeugen von *Images* der Festplatten konzentrieren. Die beiden dazu möglichen Werkzeuge gehen dabei unterschiedlich vor: Während das Windows-Tool von Acronis mit laufendem Betriebssystem arbeitet (Hotbackup), wird das Linux-Tool dd zusammen mit einem Live-System verwendet (Coldbackup). Sie entscheiden sich für eine der beiden Methoden!

2.1.1 Was ist ein Abbild?

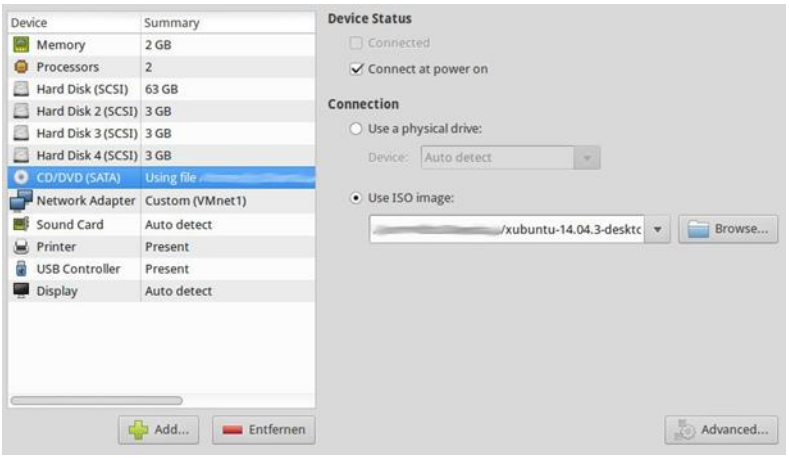
Ein Abbild (Englisch: Image) ist eine 1:1 (d.h. Bit-für-Bit) identische Kopie eines Datenträgers. Nach Erstellung ist das Ab- bild in einer normalen Datei abgelegt. Sie kennen dies vermutlich bereits von der CD: Ein Abbild einer CD wird ISO-Datei genannt. Die ISO-Datei enthält die komplette CD und ist somit eine «virtuelle» CD. Bei Festplatten ist dies nicht anders, es hat sich aber keine Dateiendung wirklich durchgesetzt. Üblich, bzw. zutreffend ist aber die Benennung als IMG-Datei (von engl. Image).

2.2 Live-System oder Notfallmedium mit «VMware Player» starten

Der Restore eines Backups ist immer dann sehr einfach, wenn das Betriebssystem selbst nicht betroffen ist. Meist ist das Backup-Programm auf dem System installiert und der Restore wird «per Knopfdruck» ausgeführt. Aber:

Wenn das Betriebssystem beschädigt ist, können Sie dieses u.U. nicht mehr hochfahren. Das von Ihnen installierte Backup- Programm lässt sich dann ebenfalls nicht mehr starten!

Für diesen Fall benötigen Sie ein vorher vorbereitetes «Notfallmedium», früher oft «Rettungsdiskette» genannt. Oder Sie booten ein «Live-System» und führen von dort die Reparatur aus. In beiden Fällen müssen Sie das «Rettungs-Image» im VMPlayer-Menü vorher einbinden:



Fügen Sie in der VMX-Datei mittels einem Texteditor ebenfalls diese Option ein:

bios.bootDelay = "5000"

Drücken Sie beim nächsten Start F2 und ändern Sie die Bootreihenfolge so, dass das CD-Laufwerk zuoberst ist. Beim nächsten Systemstart sollte nun Ihr Rettungs-System booten.

Achten Sie darauf, dass Ihre VM genug Memory zur Verfügung hat! Dies ist evtl. nicht der Fall. Passen Sie die Memory-Einstellungen an, falls Sie unter 1.5GB konfiguriert haben.

2.3 Auswahl praktische Übung

Bei der «Systemsicherung» können Sie sich ein Thema auswählen. Es machen somit nicht alle das Gleiche! *(An der Prüfung wird es zu beiden Themen Fragen haben. Sie dürfen dann aber nur zu einem Thema die Frage beantworten.)*

Aufgabe 1)

Schauen Sie sich die Übersicht der Themen an. Wählen Sie ein Thema welches Sie interessiert. Falls die Informationen der Tabelle nicht ausreichen, können Sie auch weiter hinten kurz die entsprechenden Kapitel überfliegen.

Thema	Skills / Technologie	Beschreibung
Disk-Image mit dd	Linux, Shell, Live-System, Opensource	Nutzen Sie Linux-Standard Tools um *beliebige* Systeme (Linux, Mac oder Windows) komplett zu sichern. Hierzu wird ein Abbild der gesamten Platte oder Partition erstellt.
Acronis True Image (30 Tage Testversion)	Windows, Proprietär / Closed-Source	Nutzen Sie die in Schweizer Firmen häufig eingesetzte Software zur Systemsicherung der Firma Acronis. Nur für Windows. *Registrierung mit Email und eigene USB-Disk nötig!*

Nehmen Sie möglichst eine VM mit kleinen (virtuellen) Festplatten. Wenn Sie bei der Auswahl nicht acht geben, müssen Sie schnell mal 30 Gigabyte sichern! Vorschlag:

- **Linux (dd):** Sichern sie den bisher verwendeten Applikationsserver (*vmLS3*). Das Image sollte ca. 5,4 GB gross sein und gerade noch in *bmLP1* abgelegt werden können.
- **Windows (Acronis):** *vmWP1* oder *vmWP2* benötigen etwa 20GB für das Backup.

Machen Sie in Ihrer gewählten VM vor der Sicherung einige Änderungen in System- und Nutzer-Ebene! Sonst können Sie nachher das Restore nicht verifizieren. Ändern Sie eine systemweite Konfiguration und legen Sie ein paar Nutzerdaten an.

Aufgabe 2)

1. Wählen Sie eine VM aus, welche Sie sichern wollen: ……
2. Verändern Sie die VM:
   - installieren Sie Software
   - legen Sie Benutzer an
   - erzeugen Sie Dateien
3. Sichern Sie die VM mit Ihrem gewählten Verfahren.
4. Zerstören Sie die VM, löschen Sie z.B. System-Dateien. Testen Sie: Das System darf nicht mehr starten!
5. Stellen Sie das System mithilfe Ihres Backups wieder her.

2.4 Disc-Image mit dd

Lernziele

› Systemabbild mit dd über ssh in Datei schreiben können.

2.4.1 Allgemeines Vorgehen

Sie müssen (grob) die folgenden Schritte durchführen:

1. Bootbares Live-System besorgen welches dd installiert hat (als ISO-Datei). Beispielsweise xubuntu (auf sh-smartlearn).
2. vmplayer so einrichten, dass Sie die ISO-Datei booten können.
3. Live-System booten, Tastatur und Netzwerk konfigurieren.

4. Name der Festplatte oder Partition herausfinden, z.B. mit sudo fdisk -l (nicht mounten!).
5. Festplatte oder Partition mit dd nach Ziel kopieren (z.B. auf bmLP1).

2.4.2 Einführung in dd

dd ist ein typisches Linux-Tool: es kann nur sehr wenig, ist aber gerade deshalb sehr mächtig! Die Hauptfunktion von dd ist Daten einzulesen und auszugeben. Die eingelesenen Daten können durch dd manipuliert werden, bevor sie wieder ausgegeben werden. Diese Funktionalität wird aber hier nicht benötigt. Zum Einlesen kann die Option if (in-file) gesetzt werden, zur Ausgabe wird das Argument of (out-file) gesetzt. Dies kann z.B. so aussehen:

```
# Einlesen von test.txt und ausgeben in pingu.txt
dd if=/home/vmadmin/test.txt of=/tmp/pingu.txt
```

Dies scheint noch ziemlich nutzlos zu sein, denn eine Datei lässt sich mit cp doch viel einfacher kopieren Es lassen sich aber auch ganze Laufwerke angeben, dann wird das ganze Laufwerk kopiert! Die Laufwerke heissen bei Linux meist /dev/sd und ein Buchstabe, also z.B. /dev/sda für das erste Laufwerk:

```
# Spiegle Laufwerk A nach B
dd if=/dev/sda of=/dev/sdb
```

dd kann noch viel mehr! Statt ein Laufwerk in ein anderes zu spiegeln, lässt es sich auch in eine IMG-Datei schreiben oder direkt über ssh an einen anderen Server schicken. Schauen Sie ein bisschen im Internet herum!

Hier ein Beispiel welches direkt über SSH ein komprimiertes Image erstellt:

```
sudo -i # Root werden
dd if=/dev/sda | gzip | ssh user@server 'dd of=sda.img.gz' # Backup
ssh user@server 'dd if=sda.img.gz' | gunzip | dd of=/dev/sda # Restore
```

2.5 Acronis True Image

Lernziele

- Sich in «Acronis True Image» grafisch zurecht finden.
- Ein Systembackup machen.
- Ein Restore machen.
- Mit Notfallmedium arbeiten.

Für diese Übung benötigen Sie ca. 15GB externen Speicherplatz, z.B. in Form eines USB-Laufwerks. Sie müssen diese Medien selbst organisieren.

Wenn Sie dies nicht aufbringen können, wählen Sie die andere Übung!

Acronis wartet und veröffentlicht seine Software unabhängig von diesen Lernunterlagen! Orientieren Sie sich (falls nötig) auch auf der Webseite des Herstellers über das aktuelle Vorgehen.

Aufgabe 3)

Gehen Sie auf die Webseite des Hersteller «Acronis» und besorgen Sie sich die Testversion des Produktes «Acronis True Image». Sie können die Testversion unter folgendem Link herunterladen:

http://www.acronis.com/de-de/personal/computer-backup/ (16.4.2016)

Die Datei heisst AcronisTrueImage2016_web. Installieren Sie diese auf dem Windows-System welches Sie sichern wollen.

Aufgabe 4)

Suchen Sie die Dokumentation zum Produkt und versuchen Sie ein Backup zu erstellen. Die Dokumentation zu «Acronis True Image 2016» befindet sich hier: http://www.acronis.com/de-de/support/documentation/ATI2016/#22735.html (27.10.2015)

Aufgabe 5)

Was für Backup-Quellen können Sie wählen?

.....

.....

Aufgabe 6)

Was für Backup-Ziele können Sie wählen?

.....

.....

Aufgabe 7)

Wie können Sie Ihr Backup verschlüsseln?

.....

.....

Aufgabe 8)

Führen Sie eine Systemsicherung des kompletten Systems durch. Sie benötigen dafür ca. 20 GB an Speicherplatz!

Aufgabe 9)

Erstellen Sie ein bootfähiges Medium (Acronis Notfallmedium, siehe Online-Handbuch). Sie brauchen dazu keinen USB-Stick, es reicht eine ISO-Datei zu erstellen.

Warum brauchen Sie dieses Notfallmedium? Sie haben doch schon ein Backup gemacht! Tipp: Überlegen Sie sich, wie sie

.....

3 LB2: Prüfung Theorie

Dieses Arbeitsblatt soll Sie in der Vorbereitung für die zweite Leistungsbeurteilung (LB2) unterstützen. (Bindend bleiben aber die LBV und die Angaben der Lehrperson!)

Es kommt nichts zu Backup-Kommandos (wie `tar`, `scp`, …). (Wenn Sie die Systemsicherung mit `dd` gemacht haben, ist das Kommando natürlich relevant)


Viel Glück bei den Vorbereitungen! 

3.1 Lernziele

Lernziele

- Sich in Lernumgebung (Fallbeispiel) zurecht finden.
- Bedeutung von Daten und deren Verlust benennen können.
- Mindestens drei Ursache-Kategorien von Datenverlust mit Beispiel aufzählen können.
- Relevanz eines Datensicherheitskonzeptes formulieren.
- Thematische Punkte eines Datensicherheitskonzeptes aufzählen und zuordnen.
- Vollsicherung beschreiben, unterscheiden und erkennen.
- Problematik der Dateiattribute kennen und verstehen.
- Einfaches Datensicherheitskonzept für eine Vollsicherung erstellen.
- Speicherverlauf und Anforderung einer Vollsicherung abschätzen.
- Vor- und Nachteile einer Vollsicherung benennen.
- Differenzielle Sicherung beschreiben, unterscheiden und erkennen.
- Vorteile, Nachteile und Unterschiede der Differenziellen zur Vollsicherung erklären.
- Benennen welche Deltas/Sicherungen zur Wiederherstellung gebraucht werden.
- Problematik von gelöschten Dateien im Backup-Vorgang formulieren.
- Inkrementelle Sicherung beschreiben, unterscheiden und erkennen.
- Vorteile, Nachteile und Unterschiede der Inkrementellen zu Voll- und Differenzieller Sicherung erklären.
- Grundlegende Schritte einer Wiederherstellung nennen.
- Einen Speicher für ein Backup anhand von Kriterien auswählen.
- Typen von Speicher in Hierarchie einordnen.
- Begriffe erkennen und erklären.
- Die drei Wechselalgorithmen beschreiben und erkennen.
- Aufbewahrungsdauer für die drei Wechselschemas berechnen.
- Funktion und Nutzen eines Systemabbilds beschreiben.
- Eine der zwei vorgeschlagenen Systemsicherungen kennen und umsetzen.

3.2 Begriffe

Begriff	Eigene Notizen	Kapitel
Abbild (Speicher)		13
Alterung (Datenverlust)		1
Anbindung (Speicher)		10
Applikationsserver		1
Archiv (Daten)		6
Archive Tier		10
Attribut (Datei)		3
Aufbewarung (von Daten)		2
Backup		1
Backupserver		1
Bedarf (Speicher)		4
Berechtigung (Daten)		
Bereinigen (Daten)		8
Bestand (Daten)		3
Capacity Tier		10

Cloud		10
Coldbackup		13
DAS		10
Dateiaum		8
Datei		
Datenbeständigkeit		1
Datenrettung		6
Datensicherheit		1
Datensicherheitskonzept		2
Datenverlust		1
DDR-SDRAM		10
Delta (Daten)		6
Differenziell (Sicherung / Backup)		5
DMZ		1
FIFO		12
flüchtiger Speicher		10
Fullbackup		3
Gewalteinwirkung (Datenverlust)		1
Grossvater-Vater-Sohn		12
Halbleiter Speicher		10
Hardlink		7
Hash (von Daten)		6
Heimverzeichnis (Linux)		7
Hierarchie (Speicher)		10
Hotbackup		13
Image (Speicher)		13
Informationsgesellschaft		1
Inkrementelle (Sicherung/Backup)		7
Integrität (Daten)		6
Kapazität (Speicher)		10
Konsistent (Daten/Dateisystem)		8
Kontrolle (Daten/Applikation)		8
Kopie (Daten)		3
linear (Speicherverlauf)		4
Live-System (Betriebsystem)		13
Magnetischer Speicher		10
Mechanischer Speicher		10
Medium (Speicher)		12
Metadaten		7

Vermissen Sie einen Begriff im Glossar? Haben Sie ergänzende Kapitel-Verweise? Melden Sie sich bei der Lehrperson, damit wir Ihren Vorschlag im Glossar aufnehmen können.

Vielen Dank für Ihre Mithilfe!