Hochschule für Technik, Wirtschaft und Kultur Leipzig
Fakultät für Informatik, Mathematik und Naturwissenschaften

Prüfungsprojekt für das Modul
Netzwerk- & Systemmanagement

Konzeption und Umsetzung eines Backup-Systems

B.Sc. Christof Pieloth

1. März 2011

Inhaltsverzeichnis

1 Einleitung

Als Backup wird der Vorgang einer Datensicherung sowie diese selbst in Form von digitalen Daten bezeichnet. Ein Backup-System stellt den lesenden und schreibenden Zugriff auf Speicherkapazität für diesen Zweck zur Verfügung. Die gesicherten Daten müssen ohne Verlust über viele Jahre verfügbar sein. Die konkreten Abläufe, Zeiträume, verwendeten Dateiformate und mehr werden in einem Sicherungskonzept erarbeitet. Die Betrachtung eines einzelnen Backup-Systems ist für ein vollständiges Sicherungskonzept unzureichend, da hierfür mehrere Aspekte und deren Zusammenspiel untersucht werden müssen.

Dennoch beschriebt die vorliegende Arbeit nur die Planung und Umsetzung eines Backup-Systems. In einer Vorbetrachtung werden die Themen Dateiserver, RAID, Dateifreigabe und Betriebssysteme untersucht, um eine Auswahl für das Backup-System zu treffen. Anschließend wird detailliert beschrieben wie ein Dateiserver mit der Linux-Distribution Ubuntu Server Edition 10.04 eingerichtet wird. Weiterhin wird die Erstellung und Verwaltung eines Software-RAID im RAID Level 1 für diesen Server beschrieben. Die Zugriffsrechte werden mit Hilfe von Benutzer und Gruppen des Betriebssystems verwaltet. Für die Dateifreigabe in einem Windows-Netzwerk wird ein Samba-Server mit Benutzerauthentifizierung eingerichtet. Zuletzt wird die Datensicherheit bei simulierten Controller- und Festplattenausfällen untersucht.

1.1 Relevanz und Anlass der Untersuchung

Den Anlass der Untersuchung gab das Ingenieurbüro für das Kfz.-Wesen von Volker Pieloth. Laut der Sachverständigenordnung der Handwerkskammer Halle (Saale) müssen alle Gutachten und sonstige schriftliche Unterlagen zehn Jahre aufbewahrt werden [Han05]. Das Ing.-Büro bewahrt diese Unterlagen zur Zeit in gedruckter Form auf. Digitale Unterlagen wie Lichtbilder oder diverse Protokolle werden auf CD-ROM gespeichert und archiviert. Da nunmehr alle Gutachten, Dokumente und Fotos in digitalen Formaten vorliegen, können diese ohne Mehraufwand, wie zum Beispiel das Einscannen von Papier-Fotos, digital archiviert werden. Somit werden die Druckkosten eingespart und der benötigte Lagerplatz entfällt.

1.2 Gegenstand der Untersuchung

Gegenstand der Untersuchung sind die Erarbeitung der geforderten Anforderungen an ein Backup-System und Möglichkeiten zur Umsetzung dieser. Hierzu werden die RAID Level 0, 1 und 5 zur Datensicherung untersucht. Weiterhin werden Vertreter der Betriebssysteme Windows, BSD-UNIX und Linux auf ihre Hardwareanforderungen und ihren Funktionsumfang begutachtet. Zur Freigabe der Daten und zur Administration werden die Netzwerkprotokolle FTP, SSH und SMB betrachtet. Diese Untersuchungen werden immer unter Berücksichtigung der zuvor erarbeiteten Anforderugen durchgeführt.

1.3 Zielsetzung

Ziel dieser Arbeit ist die praktische Umsetzung eines Backup-Systems, welches genügend Speicherkapazität und Sicherheit bietet, um Daten zuverlässig über den geforderten Zeit-

raum von zehn Jahren zu speichern. Die Daten sollen über eine Netzwerkfreigabe von Windows-Clients gesichert und auch wieder gelesen werden können. Als Ergebnis dieser Arbeit soll ein einsatzbereites technisches Gerät hervorgehen, welches die geforderten Anforderungen erfüllt.

Es ist nicht das Ziel ein Sicherungskonzept zu erarbeiten. Dies würde die Untersuchung von geeigneten Dateiformaten, Sicherungsintervallen, Synchronisationssoftware und mehr beanspruchen.

1.4 Aufbau der Arbeit

Im ersten Teil dieser Arbeit werden mögliche Technologien und Anwendungen betrachtet, um eine Auswahl für das umzusetzende System zu treffen.

Der zweite Teil beschreibt ausführlich die Installation und Konfiguration des Systems mit der zuvor erstellten Auswahl.

Hierbei werden spezielle Schreibweisen verwendet um die Übersichtlichkeit zu erhöhen. In *Kursivschrift* markierte Begriffe oder Sätze, sind von Programmen aus Menüpunkten, Auswahlen o.ä. übernommene Inhalte. Befehle, Programmausgaben und Dateiinhalte sind in `Maschinenschrift` dargestellt. Längere Passagen sind vom Fließtext gelöst und grau unterlegt:

```
echo 'hello world' >> hello.txt
cat hello.txt
```

Des Weiteren werden bei der allgemeinen Erklärung von Befehlen Variablen genutzt. Diese sind durch spitze Klammern gekennzeichnet und müssen bei der Anwendung durch einen entsprechenden Wert ersetzt werden. Der Name der Variable beschreibt deren Funktion. Zum Beispiel benötigt der Befehl zum Erstellen eines Ordners den Ordnernamen als Argument:

```
mkdir <directoryname>
```

Um einen Ordner mit dem Namen „foo" zu erstellen muss die Variable `<directoryname>` durch `foo` ersetzt werden:

```
mkdir foo
```

Werte in eckigen Klammern sind mögliche Optionen und können entweder gesetzt oder nicht gesetzt werden, wobei die Klammern bei Verwendung nicht mit angegeben werden.

2 Vorbetrachtung

In diesem Kapitel werden das Einsatzszenario und bestehende Vorbedingungen beschrieben. Anhand dieser Informationen werden benötigte Anforderungen an das System formuliert. Abschließend werden Technologien und Anwendungen diskutiert, welche die Anforderungen für das Einsatzgebiet am besten erfüllen und für die Umsetzung genutzt werden sollen.

2.1 Szenario

Das Ing.-Büro sichert und archiviert derzeit monatlich alle anfallenden Gutachten. Dieser Rhythmus soll bei dem Backup-System beibehalten werden. Jährlich werden durchschnittlich 800 Versicherungsgutachten und 20 Gerichtsgutachten erstellt. Versicherungsgutachten benötigen mit dem Gutachten, Fotos und Schriftverkehr ca. 55MB. Gerichtsgutachten benötigen ca. 200MB. Der jährliche Speicherbedarf beträgt somit:

$$800 \cdot 55\text{MB} + 20 \cdot 200\text{MB} = 48000\text{MB}$$

Da erst nach 11 Jahren die ersten Daten gelöscht werden können, beträgt der gesamte Speicherbedarf des Backup-Systems:

$$48000\text{MB} \cdot 11 = 528000\text{MB} \approx 528\text{GB}$$

Der Speicherbedarf von 528GB kann allerdings nur als ein Minimum angenommen werden, da bei dieser Rechnung nicht berücksichtigt wurde, dass neue Dateiformate oft mehr Speicherbedarf benötigen als ihre Vorgänger. Ein unformatiertes A4-Dokument verbraucht als ASCII kodierte Textdatei nur 2,8KB. Hingegen benötigt das selbe Dokument im OpenDocument-Text-Format schon 7,5KB. Diese Entwicklung kann eingeschränkt werden, indem für die Langzeitarchivierung standardisierte Dateiformate festgelegt und genutzt werden. Des Weiteren bietet eine physische Sicherung nicht genügend Sicherheit vor höherer Gewalt. Diese und andere Überlegung erfordern jedoch die Erarbeitung eines Sicherungskonzeptes, welches nicht Bestandteil dieser Arbeit ist.

Aufgrund der monatlichen Sicherung kann das System während der nicht genutzten Zeit ausgeschaltet bleiben. Dies verringert die Betriebszeit und damit auch das Ausfallrisiko der verwendeten Hardware. Der Sicherungsvorgang wird von einem Windows-Client über ein 100-Mbit/s-Ethernet durchgeführt. Die Daten auf dem System müssen auch nach einem Teilausfall des Systems, zum Beispiel den Ausfall einer Festplatte oder des Speichercontrollers, rekonstruierbar sein.

Da ein neuer Desktop-PC für die Firma angeschafft wurde, steht die alte Hardware für dieses System zur Verfügung. Diese hat die folgenden Leistungsmerkmale:

Prozessor AMD Athlon(tm) XP 1600+ (1400MHz)

Mainboard Gigabyte GA-7DXR

Hauptspeicher 768MB (200MHz) DDR-SDRAM

Festplatte Hitachi Deskstar IC35L040AVVN07-0 (40GB, ATA/IDE)

Grafikkarte Gainward Geforce 2 TI (64MB)

Netzwerkkarte D-Link DFE-530TX

2.2 Anforderungen

Aus dem zuvor beschriebenen Szenario ergeben sich diese Anforderungen:

1. Das System benötigt eine Speicherkapazität von mindesten 528GB zuzüglich der benötigten Kapazität des Betriebssystems und anderer Programme.
2. Es dürfen keine Daten verloren gehen, wenn
   a) ein Speichercontroller und/oder
   b) eine Festplatte und/oder
   c) beliebige andere Komponenten ausfallen.
3. Auf das Backup-System muss mit einem Windows-Client über ein 100-Mbit/s-Ethernet zugegriffen werden können.
4. Das System muss ohne angeschlossene Ein- und Ausgabegeräte (Bildschirm, Tastatur, Maus) konfigurierbar und wartbar sein („Headless-Workstation").

2.3 Network Attached Storage oder Fileserver

Für die beschriebene Aufgabe bieten sich zwei Systeme an:

1. Network Attached Storage (kurz: NAS)
2. Computer als Fileserver

Als NAS-System, zu deutsch „an das Netzwerk angeschlossener Speicher", werden Geräte bezeichnet, die ohne hohen Konfigurationsaufwand Speicherkapazität in einem Rechnernetz bereitstellen. Diese Systeme verwenden auf das Einsatzgebiet spezialisierte und zugeschnittene Hardware und Software. Für den Heimbereich beschränkt sich die Hardwareauswahl oft auf die nötigsten Komponenten um Strom und Materialkosten zu sparen. Die Leistung der Komponenten reicht meist gerade für den Einsatzzweck aus. Die Software ist genau auf das System zugeschnitten und beinhaltet einen minimierten Betriebssystemkern, Netzwerkdienste für den Datenzugriff und eine Weboberfläche für die Konfiguration.

Der Server ist ein Computer, der den Netzwerkbenutzern im Rahmen eines Client-Server-Modells Dienste und Ressourcen zur gemeinsamen Nutzung zur Verfügung stellt. Die benötigte Leistung ist von den bereitgestellten Diensten und der zu bedienenden Anzahl von Clients abhängig. Im vorliegendem Szenario sind die bereitgestellte Speicherkapazität und die maximale Übertragunsrate im 100-Mbit/s-Ethernet relevant.

Aufgrund der reduzierten und spezialisierten Hardware eines NAS-Systems ist der Stromverbrauch geringer als der eines Servers. So verbraucht zum Beispiel das System „ReadyNAS Duo" von Netgear laut Herstellerangaben 35W [Net]. Nach eigenen Messungen verbraucht der zur Verfügung stehende Computer ohne Rechenlast 117W. Da das Backup-System nur während des Sicherungsvorgangs in Betrieb ist, kann das NAS-System diesen Vorteil nicht voll auskosten.

Um einen Datenverlust bei einem Festplattenausfall vorzubeugen, kann auf beiden Systemen in der Regel ein RAID eingerichtet werden. Ein RAID ist ein Verbund von mehreren Festplatten um einen Datenverlust bei Festplattenausfall zu vermeiden und die Performance zu erhöhen. Diese Technologie wird genauer in Kapitel 2.4 erläutert. Laut

den Anforderungen aus Kapitel 2.2 müssen die Daten auch nach dem Ausfall beliebiger Komponenten rekonstruierbar sein. Dies kann bei proprietärer Hard- und Software nicht mit vollständiger Sicherheit vorausgesagt werden. Fällt zum Beispiel der Speichercontroller eines NAS-Systems aus, ist eine Neuanschaffung des Gerätes nicht ausgeschlossen! Ob der Hersteller dieses Modell auch in zehn Jahren noch vertreibt, ist fraglich. Ein Server bietet die Möglichkeit die Hardware und Software auf diese Fähigkeiten hin zu untersuchen. Zusätzlich muss bei defekter Hardware des Servers nicht das gesamte System gewechselt werden, sondern es genügt die defekte Komponente zu tauschen.

Die noch ausstehenden Anforderungen, die benötigte Speicherkapazität, Netzwerkzugriff eines Windows-Clients und der Headless-Betrieb, können von beiden System erfüllt werden. Aufgrund des voll funktionsfähigen Betriebssystems eines Servers können neue Dienste für spätere Anforderungen eingerichtet werden. Hingegen bietet ein NAS-System nur die im Lieferumfang enthaltenen Funktionen.

Zusammenfassend bieten ein NAS-System und ein Server für das vorliegende Szenario ähnliche Funktionen. Da ein Datenverlust bei einem NAS-System nicht vollständig ausgeschlossen ist und bereits ein Computer zur freien Verfügung steht, wird ein Fileserver zur Umsetzung gewählt.

2.4 Redundant Array of Independent Disks

Dieser Abschnitt definiert den Begriff „RAID" und diskutiert anschließend die verschiedenen Möglichkeiten der Umsetzung. Als Grundlage dienen die Ausführungen von Andrew S. Tanenbaum aus dem Buch „Computerarchitektur" [Tan06].

Redundant Array of Independent Disks (kurz: RAID), zu deutsch „redundante Anordnung unabhängiger Festplatten", ist ein Verbund mehrerer physischer Festplatten zu einem logischen Laufwerk. Zwei grundlegende Ziele eines RAID sind die Performancesteigerung und die Erhöhung der Ausfallsicherheit. Um diese Ziele zu erreichen werden die Daten über die Einzellaufwerke verteilt. Für solch einen Verbund können verschiedene Organisationsformen, sogenannte RAID Level, mit unterschiedlichen Methoden der Verteilung gewählt werden. Grundsätzlich kann zwischen den RAID Level 0 bis 5 unterschieden werden, wobei mit der Zeit weitere RAID Level entwickelt wurden, die die Vorteile mehrerer „Grund-RAID-Level" vereinen. In den folgenden Abschnitten werden nun drei RAID Level betrachtet, welche die wichtigsten Organisationsformen verdeutlichen. Des Weiteren wird der Unterschied zwischen einen Software- und Hardware-RAID beschrieben.

2.4.1 RAID Level 0

Das RAID Level 0 wird aufgrund der Art der Datenverteilung als Striping, zu deutsch „in Streifen zerlegen", bezeichnet. Hierbei wird die virtuelle Festplatte in sogenannte Strips (Streifen) der Größe von k Sektoren zerlegt. Der Strip 0 beinhaltet somit die Sektoren 0 bis $k-1$, der Strip 1 die Sektoren k bis $2k-1$ usw. Diese Strips werden aufeinander folgend zyklisch auf die Laufwerke verteilt. Der RAID-Controller übernimmt die Aufgabe der Zerteilung des Datenstroms in Strips, sowie das korrekte Zusammensetzen im Speicher und stellt sicher, dass die Befehle an die einzelnen Laufwerke in der richtigen Abfolge versendet werden. Für dieses RAID Level werden mindestens zwei Laufwerke benötigt. In Abbildung 2.1 ist diese Verteilung des Datenstroms auf vier Laufwerke dargestellt.

Das Striping ermöglicht es, beliebig viele Laufwerke zu einem logisch zusammenhängenden Speicherbereich zusammenzufassen. Die maximale Kapazität eines RAID Level 0 ergibt sich aus dem Produkt der Speicherkapazität des kleinsten Laufwerks und der Anzahl der Laufwerke:

$$Kapazität = MIN(Kapazitäten\,der\,Laufwerke) \cdot Anzahl\,der\,Laufwerk$$

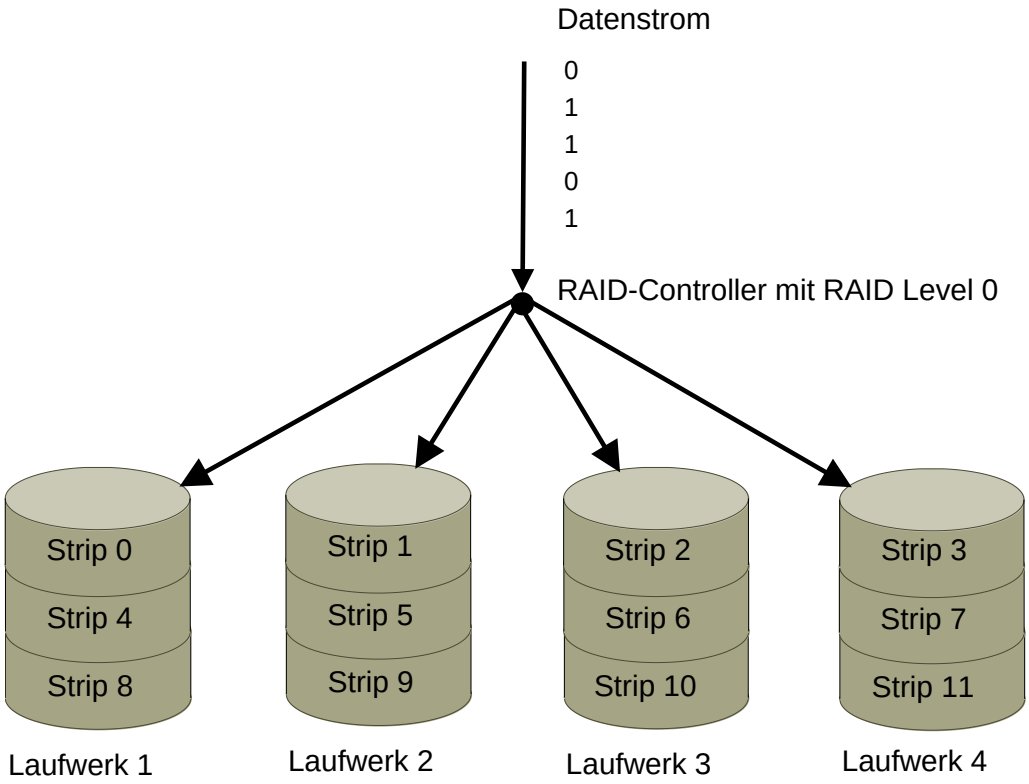

Abbildung 2.1: Datenverteilung eines RAID Level 0 mit vier Laufwerken.

Falls ein Datenblock gelesen werden soll, der in aufeinander folgenden Strips gespeichert ist, kann diese Anfrage parallel verarbeitet werden. Dadurch kann bei Datenabfragen mit einer Größe von mindestens $2k$ eine höhere Leistung als bei einer einzelnen Festplatte erzielt werden.

Jedoch kann bei dieser Organisationsform eigentlich nicht von einem echten RAID gesprochen werden, weil keine Redundanz vorhanden ist. Bei dem Ausfall von nur einem Laufwerk können keine Daten mehr erfolgreich zusammengesetzt werden und sind somit verloren. Zusätzlich sinkt der mittlere Ausfallabstand mit jedem weiteren Laufwerk![1] Der mittlere Ausfallabstand, auch Mean-Time-Between-Failure (kurz: MTBF) genannt, ist der Quotient aus der Summe der Betriebszeiten und der Summe der Ausfälle eines Bauteils:

$$MTBF = \frac{\sum Betriebszeit\,in\,Stunden}{\sum Ausfälle}$$

Da die Betriebszeiten der Laufwerke in einem Verbund im RAID Level 0 die gleichen sind, sich jedoch die Anzahl der Ausfälle erhöhen, sinkt der mittlere Ausfallabstand. Angenommen für eine Festplatte traten während der Betriebszeit von 100.000 Stunden zwei Ausfälle auf. So ist die MTBF:

$$MTBF = \frac{100.000h}{2} = 50.000h$$

Bei einem RAID 0 mit zwei Laufwerken des selben Typs könnten während der Betriebszeit von 100.000 Stunden insgesamt vier Ausfälle auftreten. Somit sinkt die MTBF auf:

$$MTBF = \frac{100.000h}{4} = 25.000h$$

Neben der fehlenden Redundanz, verschlechtert sich auch zusätzlich die Zuverlässigkeit!

[1] Der MTBF sinkt bei jedem RAID Level.

2.4.2 RAID Level 1

Als Mirroring, zu deutsch Spiegelung, wird das RAID Level 1 bezeichnet. Für diese Organisationsform werden mindestens zwei Laufwerke benötigt, da jedes Strip autmatisch auf mindestens zwei Laufwerke geschrieben wird. Durch diese Redundanz kann diese Organisationsform als echtes RAID bezeichnet werden. Bei einem Lesevorgang wird eine der Kopien genutzt und die Belastung verteilt sich auf alle Laufwerke. Aufgrund der zusätzlichen Kopien sind alle Daten nach einem Ausfall weiterhin vorhanden. Es muss lediglich das defekte Laufwerk getauscht und die Daten von der funktionsfähigen Festplatte auf die neue synchronisiert werden. Im Gegensatz zu einem RAID Level 0 ist die Speicherkapzität der Quotient aus der Summe aller Laufwerke und der Anzahl der Kopien:

$$Kapazität = \frac{\sum Kapazität\,der\,Laufwerk}{Anzahl\,der\,Kopien}$$

Es geht also Speicherkapazität auf Kosten der Redundanz verloren!

Wenn mindestens vier Laufwerke genutzt werden, kann bei einer geraden Anzahl das Striping mit dem Mirroring kombiniert werden. Somit wird eine Fehlertoleranz mit gesteigerter Leistung erzielt. Die Fehlertoleranz, also die Anzahl möglicher Festplattenausfälle ohne Datenverlust, ergibt sich aus der Anzahl der Kopien subtrahiert mit 1. In Abbildung 2.2 ist ein RAID Level 1 mit vier Laufwerken dargestellt. Hierbei werden die Laufwerk 1 und 2 im RAID Level 0 betrieben. Die Strips dieses Verbunds werden auf die Laufwerke 3 und 4 „gespiegelt". In diesem Beispiel existieren zwei Kopien und somit darf maximal eine Festplatte ausfallen ohne einen Datenverlsut zu erleiden. Angenommen das Laufwerk 2 ist defekt, kann die Kopie von Laufwerk 4 gelesen werden. Fallen jedoch die Laufwerke 1 und 3 aus, können keine Daten erfolgreich zusammengesetzt werden.

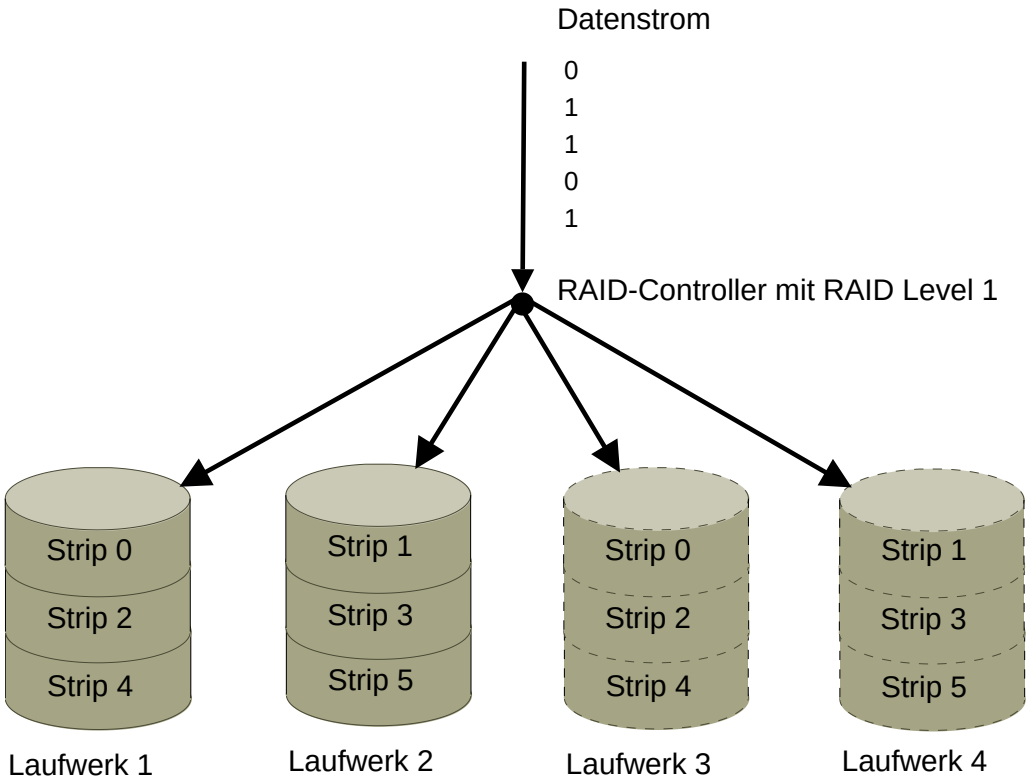

Abbildung 2.2: Datenverteilung eines RAID Level 1 mit vier Laufwerken.

2.4.3 RAID Level 5

Durch die Bildung der Parität kann ebenfalls eine Redundanz erzielt werden. Diese Möglichkeit wird von mehreren RAID Level genutzt, soll aber an dieser Stelle nur anhand des RAID Level 5 gezeigt werden. Diese Organisationsform ermöglicht eine Leistungssteigerung und schützt vor dem Ausfall einer Festplatte bei nur geringen Verlust der nutzbaren Speicherkapazität. Diese Beträgt maximal:

$$Kapazität = \\ (Anzahl\,der\,Laufwerke - 1) \cdot MIN(Kapazitäten\,der\,Laufwerke)$$

In Abbildung 2.3 ist das RAID Level 5 mit vier Laufwerken verdeutlicht. Dieses arbeitet ebenfalls mit Strips von denen eine Parität der Größe k Sektoren zur Ausfallsicherheit gebildet wird, d.h. die Strips werden `XOR` miteinander verknüpft. Das Paritäts-Strip wird hierbei zyklisch auf alle Laufwerke verteilt. Wenn nun eine Festplatte ausfällt, nimmt der RAID-Controller für das fehlende Bit eine 0 an. Falls bei dieser Annahme die gespeicherte Parität nicht mit der errechneten übereinstimmt, muss das fehlende Bit 1 gewesen sein. Aufgrund der Parität und deren zyklischen Verteilung ist die Rekonstruktion des defekten Laufwerks ein aufwendiger und komplexer Vorgang.

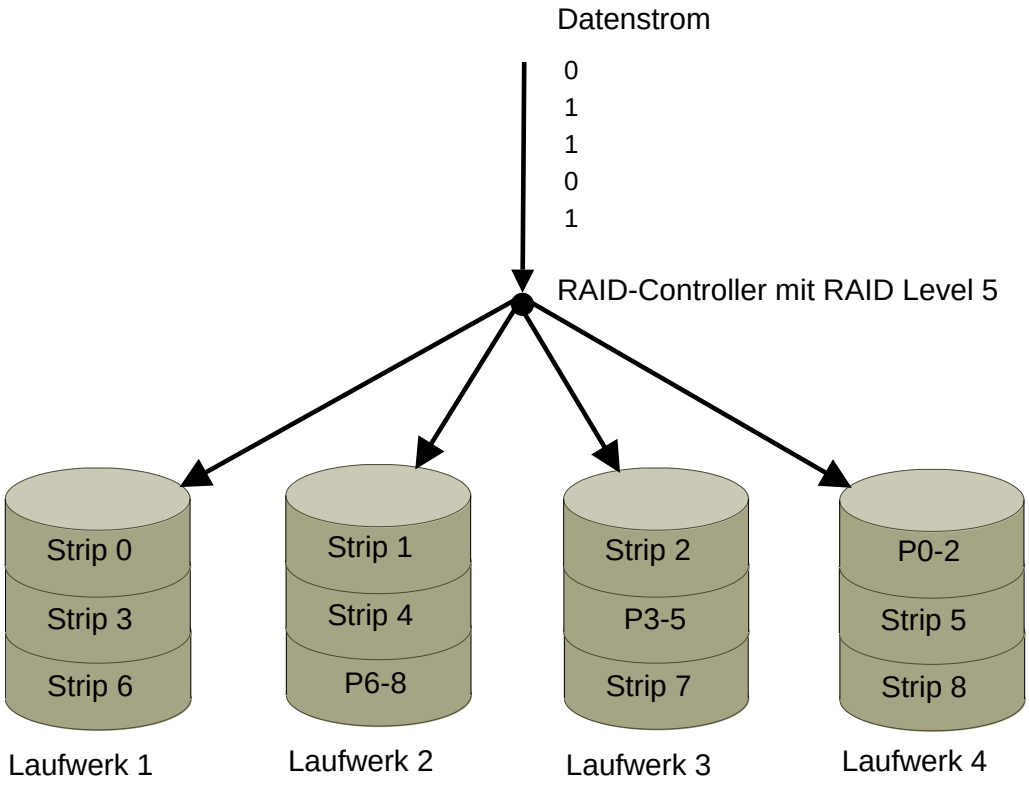

Abbildung 2.3: Datenverteilung eines RAID Level 5 mit vier Laufwerken.

2.4.4 Software- & Hardware-RAID

Ein RAID-Controller kann entweder über eine spezielle Software oder Hardware realisiert sein.

Bei einem sogenannten Software-RAID werden die Logik der verschiedenen Organisationsformen vom Hauptprozessor berechnet. Dadurch kann die vorhandene Hardware, wie zum Beispiel ein Onboard-Speichercontroller eines Mainboards, genutzt werden, um die angeschlossenen Laufwerke zu einem RAID-Verbund zusammenzuschließen. Jedoch beansprucht jeder Lese- und Schreibvorgang Rechenzeit, wodurch die Gesamtperformance eines Computers sinkt.

Ein sogenanntes Hardware-RAID hat diesen Nachteil nicht, da die Logik von spezieller Hardware berechnet wird. Somit wird der Hauptprozessor von der Last der RAID-Verwaltung entlastet. Diese Hardware kann zum Beispiel über eine PCI-Karte nachgerüstet werden. Aufgrund der proprietären Hardware ist jedoch nicht sichergestellt, dass ein bestehender RAID-Verbund, im Falle eines Hardwaredefekts, von einem anderen RAID-Controller ausgelesen werden kann. Wie bei einem NAS-System besteht hier das Risiko, dass dieser RAID-Controller in zehn Jahren nicht mehr verkauft wird. Im Unterschied dazu ist es in der Regel möglich, zum Beispiel eine Festplatte aus einem Software-RAID mit dem Level 1 an einem beliebigen Speichercontroller als Einzellaufwerk auszulesen.

2.4.5 Auswahl

Um die zweite Anforderung aus Kapitel 2.2 zu erfüllen, benötigt das zu konzipierende System ein RAID. Da das RAID Level 0 keine Redundanz bietet, ist es für die beschriebene Datensicherung ungeeignet. Leistungsteigerung und Sicherheit sprechen für das RAID Level 5, jedoch können die Daten nur sehr aufwendig und nicht an einem beliebigen Speichercontroller rekonstruiert werden. Somit fällt die Wahl auf das RAID Level 1, da hier jedes beliebige Laufwerk ein vollständig nutzbares Dateisystem enthält.

Weil der Backup-Server für keinen kritischen Geschäftsprozess benötigt wird, hat die Datensicherheit eine höhere Priorität als die Performance. Aufgrund dessen wird ein Software-RAID verwendet, um eine Datenwiederherstellung bei defekter Hardware zugewährleisten.

2.5 Bereitstellung der Speicherkapazität

Die Datensicherung sowie der Zugriff auf bereits gesicherte Daten muss von einem Windows-Client über ein 100-Mbit/s-Ethernet möglich sein. Der Inhalt bereits gesicherter Dateien ist unveränderlich. Aufgrund der bestehenden Arbeitsabläufe sind die Daten vor der Sicherung in einer Ordnerstruktur vorsortiert. Dadurch kann auf spezielle Software für Datensicherung und Synchronisation verzichtet werden und es wird lediglich der Zugriff über ein Netzwerk benötigt.

Um den Speicherplatz bereitstellen zu können, stehen unter Berücksichtigung der Anforderungen folgende Netzwerkprotokolle zur Verfügung:

- File Transfer Protocol (kurz: FTP)
- SSH File Transfer Protocol (kurz: SFTP)
- Server-Message-Block-Protokoll (kurz: SMB)

Das File Transfer Protocol, zu deutsch „Dateiübertragunsprotokoll", ist ein Protokoll zur Übertragung von Dateien in einem Rechnernetz. Es wurde 1985 im Request For Comments 959 [PR85] spezifiziert. Bei diesem Protokoll findet die Kommunikation über zwei Verbindungen, der „Data Connection" und der „Control Connection", statt. Die Control

Connection nutzt das Telnet Protokoll [PR83] um Befehle zu übertragen, die zum Beispiel eine Datenübertragung über die Data Connection starten. Für beide Protokolle, sowohl das FTP als auch Telnet, sind keine verschlüsselte Datenübertragung und Authentifizierung spezifiziert. Trotz dieser Einschränkung ist FTP bis heute im Internet stark verbreitet, unter anderem da es von allen gängigen Betriebssystemen und Browsern unterstützt wird. Aufgrund der unsicheren Authentifizierung ist das File Transfer Protocol für den Backup-Server ungeeignet!

Als Ersatz für das unsichere Telnet hat sich die „Secure Shell" (kurz: SSH) etabliert. Die Sicherheit wird in SSH durch die Authentifizierung des Servers gegenüber des Clients mit einem Zertifikat und einer vollständig verschlüsselten Kommunikation gewährleistet. Über eine bestehende SSH-Verbindung kann eine sichere Datenübertragung unter Nutzung von SFTP stattfinden. Aufgrund dieser Eigenschaften bieten sich SSH und SFTP besonders für die Administration und Datenübertragung über das Internet an. Da mit SSH sicher auf eine entfernte Kommandozeile zugegriffen werden kann, wird somit die Forderung nach einer Headless-Workstation erfüllt.

In Windows-Umgebungen kann zudem die „Datei- und Druckerfreigabe" genutzt werden. Diese verwendet das Kommunikationsprotokoll „Server Message Block". Das Sicherheitsmodell unterscheidet zwischen:

- User-level authentication (Authentifizierung auf Benutzerebene)
- Share-level authentication (Authentifizierung auf Freigabeebene)

Die Authentifizierung auf Benutzerebene ermöglicht den Zugang mit Hilfe eines Benutzernamens und eines Passworts. Diese Art ermöglicht es Freigaben speziell für Benutzer und Gruppen einzurichten. Eine Authentifizierung auf Freigabeebene fordert für den Zugang einer Ressource nur ein Passwort. Bei beiden Sicherheitsmodellen wird das Passwort verschlüsselt übermittelt [Mic10], lediglich die Datenübertragung findet unverschlüsselt statt. SMB ist somit für die Dateifreigabe für Windows-Clients in einem lokal geschützten Netzwerk geeignet.

Zusammenfassend wird SSH für die Administration, SFTP für die Datenübertragung über das Internet und SMB für die Datenübertragung in einem lokalen Netzwerk verwendet.

2.6 Betriebssysteme

Zu Beginn dieses Kapitels wird kurz der Begriff des Betriebssystems und dessen Funktionen erklärt. Anschließend wird in wenigen Worten die Entwicklung der heute verbreitesten Systeme zusammengefasst. Abschließend werden anhand eines Repräsentanten aus den Kategorien Windows, BSD-UNIX und Unixoid die unterstützten Anforderungen betrachtet, um ein Betriebssystem für die Umsetzung auszuwählen.

2.6.1 Allgemein

Das Betriebssystem ist, neben der Firmware spezieller Hardware, die unterste Software in den Abstraktionschichten eines Computers. Indem es häufig genutzte Operationen zentral für darüber liegende Programme zur Verfügung stellt, vereinfacht es die Nutzung eines Computers. Zusätzlich verwaltet es Betriebsmittel wie Speicher, Rechenzeit, Zugriff auf Geräte und mehr.

Andrew Tanenbaum bezeichnet diese Funktionen eines Betriebssystems als eine erweiterte Maschine und Ressourcenmanager [Tan02].

Obwohl in der Ebene der Maschineninstruktionen oft nur weniger als 100 Befehle für ein Gerät zur Verfügung stehen, ist die Programmierung in dieser Ebene aufgrund der spezifischen Details eines Geräts sehr schwierig. Als Beispiel sei der Datenzugriff auf

beliebige Ressourcen gewählt. Ein Programmierer muss für jeden Datenzugriff auf ein Gerät (Diskette, Festplatte, CD-ROM) eine eigene Funktion schreiben, welche jedoch immer den selben Zweck erfüllt. Für das Programmieren von Anwendungen ist es effizienter, wenn die Details hinter einer Schnittstelle verborgen bleiben. Diese Aufgabe übernimmt ein Betriebssystem, indem es dem Benutzer ein Äquivalent einer erweiterten Maschine präsentiert, welches jedoch einfacher zu programmieren ist, als die darunter liegende Hardware.

Bis Ende der 60er Jahre im 20. Jahrhundert war es üblich Programme vollständig seriell abzuarbeiten, bevor ein anderes Programm geladen wurde. Zu dieser Zeit war es die Aufgabe des Programms den Zugriff auf Geräte zu verwalten. Mit dem Wunsch nach einem Mehrbenutzer-System wurde 1957 das Konzept des „Time-Sharing" erfunden. Hierbei teilen sich Programme die vorhandene Rechenzeit eines Prozessors, wobei es für ein Programm so aussieht, als hätte es die gesamten Ressourcen zur Verfügung. Um in einen solchen Szenario einen problemlosen Betrieb zugewährleisten, müssen die Betriebsmittel und deren Nutzung durch die Programme verwaltet werden. So muss zum Beispiel jedem Programm eine bestimmte Rechenzeit zugeordnet werden, der Zugriff eines Programms auf den Speicherbereich eines anderen Programms verhindert werden und der Zugriff auf Geräte koordiniert werden. Da diese Verwaltung nur zentral gelöst werden kann, übernimmt das Betriebssystem die Ressourcenverwaltung.

2.6.2 Entwicklung

Den größten Einfluss auf die Entwicklung der Betriebssysteme, so wie sie heute bekannt sind, hatten UNIX und Windows.

UNIX wurde vorallem zur Unterstützung der Softwareentwicklung und als Mehrbenutzer-System entwurfen. Somit richtet es sich an erfahrene Programmierer, die im Gegensatz zu den meisten heutigen Desktop-Nutzern, konsistente und einheitliche Schnittstellen und weniger eine einfach zu bedienende grafische Oberfläche benötigen. Der strengen Umsetzung der Entwurfsziele und neuer Konzepte verdankt UNIX vorallem im wissenschaftlichen Umfeld seinen guten Ruf.

Da es immer schwieriger wurde UNIX vollständig zu verstehen, entwickelte Andrew Tanenbaum MINIX. Als „Mini-UNIX" sollte es die Konzepte von UNIX für Ausbildungszwecke verdeutlichen. Weil UNIX in dieser Zeit noch nicht frei verfügbar war, wurde es nach dem Erscheinen von vielen genutzt und die Erweiterungsanfragen häuften sich. Linus Torwalds entschloss sich ein weiteres UNIX-ähnliches Betriebssystem, Linux, zu entwickeln, weil nur wenig dieser Anfragen in MINIX Einzug hielten. Mit der Zeit wurden viele UNIX-Anwendung auf Linux portiert, da Linux nicht den Anspruch an ein überschaubares Betriebssystem für Ausbildungszwecke verfolgte. Linux wird als Unixoid oder UNIX-Derivat bezeichnet, weil es die Ideen, Konzepte und teilweise die API von UNIX umsetzt, jedoch nicht aus dem nativen Quellcode entstand.

1994, im Jahr der Veröffentlichung von Linux Version 1, hatte die Berkeley Software Distribution den kompletten Quellcode von UNIX neugeschrieben, sodass ein vollständiges UNIX als Open-Source verfügbar war. Alle UNIX-Versionen oder Distributionen die aus der Berkeley Software Distribution entstanden sind, werden BSD-UNIX genannt.

Anders als bei UNIX liegen die Wurzeln von Windows in einem Einzelbenutzer-System mit dem Namen „MS-DOS". Diesem wurde 1985 eine grafische Benutzerschnittstelle beigefügt (Windows 1.0), jedoch erfüllte erst Windows 95 die wichtigsten Anforderungen eines Betriebssystems wie zum Beispiel virtueller Speicher. Als Folge der Anstrengungen von Microsoft, ein modernes 32-Bit-Betriebssystem ohne „MS-DOS-Altlasten" zuentwickeln, entstand Windows NT. 1993 wurde Windows NT 3.1 veröffentlicht, welches die wichtigsten Anforderungen eines Betriebssystems erfüllte und die Basis bis zum aktuellen Windows 7 bildet. Anders als bei UNIX und dessen Derivaten befindet sich die grafische Benutzerschnittstelle bei Windows im Kernmodus. Als Folge ist ein Windowssystem über

die Kommandozeile schwieriger zu administrieren, da der Fokus auf der grafischen Oberfläche liegt. Dies ist besonders bei einer Core-Installation von Windows Server 2008 zu sehen. Diese stellt ein minimales System mit einer Befehlszeile zur Verfügung. Dennoch ist kein „purer" Befehlszeilenzugriff wie bei UNIX möglich, da die gestartete Befehlszeile ebenfalls in einem Fenster geöffnet ist und somit der Zugriff über einen Remote Desktop erfolgen muss.[2]

2.6.3 Windows, BSD-UNIX oder Unixoid

Anforderung	Windows Server 2008	Ubuntu Server 10.04	FreeBSD 8.1
Software-RAID Level 1	ok	ok	ok
100-Mbit/s- Ethernet	ok	ok	ok
Headless-Workstation/ Remote-Zugriff	RDP	Kommandozeile	Kommandozeile
SSH+SFTP	ok	ok	ok
Server-Message-Block	ok	ok	ok
Prozessor	1GHz	300MHz	486 oder besser
Hauptspeicher	512MB	128MB	24MB
Kapazität bei Standardinst.	20GB	1GB	150MB
Treiberunterstützung	sehr gut	befriedigend	ausreichend

Tabelle 2.1: Überblick der benötigten Anforderung ausgewählter Betriebssysteme.

Die Tabelle 2.1 stellt die ausgewählten Betriebssysteme unter Berücksichtigung der Anforderungen gegenüber. Für die Gruppe der Windows Betriebssysteme wurde Windows Server 2008 gewählt. Als Repräsentant einer Linux-Distribution wurde Ubuntu Server 10.04 und für BSD-UNIX FreeBSD 8.1 ausgesucht. Beide Betriebssysteme sind laut DistroWatch.com und bsdstats.org am weitesten verbreitet [Dis, BSD]. Alle betrachteten Betriebssystem unterstützen sowohl ein Software-RAID im Level 1 und ein 100-Mbit/s-Ethernet. Zusätzlich werden SSH, SFTP und SMB von allen untersützt.

Unterschiede gibt es beim Remote-Zugriff. Ein effizienter Remote-Zugriff ist bei Windows nur über einen Remote Desktop möglich, da die Administration hauptsächlich über die grafische Benutzeroberfläche erfolgt. Dies kann bei Wartungsarbeiten über eine langsame Internetverbindung zum Problem werden, da die Bildschirmübertragung wahrnehmbar verzögert werden kann.[3] Sowohl Ubuntu als auch FreeBSD lassen sich effizient über die Kommandozeile administrieren, welche auch bei langsamer Internetverbindung problemlos funktioniert. Bei Bedarf können bei beiden Betriebssystemen auch Protokolle zur Steuerung eines Desktops installiert werden.

Große Unterschiede fallen bei den Hardwareanforderungen auf. Den leistungsstärksten Computer benötigt Windows Server 2008 mit einem Prozessor mit mindestens 1GHz, 512MB Hauptspeicher und mindesten 20GB Festplattenkapazität. Dennoch würden diese Anforderungen von dem zur Verfügung stehenden System erfüllt werden. Die niedrigsten Anforderung an das System hat FreeBSD, bei einer allerdings sehr minimalistischen Installation. Aufgrund der „großen Verwandschaft" zwischen FreeBSD und Ubuntu, genauer UNIX und Linux, können für FreeBSD bei vergleichbaren Funktionsumfang ähnliche Anforderungen angenommen werden wie bei Ubuntu. Diese liegen mit einem 300MHz Prozessor, 128MB Hauptspeicher und 1GB Festplattenkapazität weit unter den Leistungsmerkmalen des verfügbaren Computers.

[2] Zusätzlich können bei einer Core-Installation auch Verwaltungsfenster geöffnet werden.
[3] Laut Meinung des Autors sind bidirektional mindestens 512Kbit/s nötig.

Da Windows-Betriebssysteme sehr weit verbreitet sind, werden in der Regel zu jedem Gerät Windows-Treiber vom Hersteller angeboten. Laut einem Vergleich auf der Website von FreeBSD bietet dieses technisch bessere Möglichkeiten für die Treiberunterstützung als Linux [BS00]. Die Erfahrung des Autors ist jedoch, dass von Linux mehr Geräte mit Treibern untersützt werden.

Zusammenfassend zeigt die Tabelle 2.1, dass alle ausgewählten Betriebssysteme die Anforderungen, teilweise mit Einschränkungen, erfüllen. Linux und BSD-UNIX haben gegenüber Windows den Vorteil, dass sie kostenfrei verfügbar sind. Aufgrund dessen und der niedrigeren Hardwareanforderungen muss zwischen Linux und BSD-UNIX entschieden werden. Grundsätzlich bieten beide Betriebssysteme für das vorliegende Szenario die gleichen Möglichkeiten. Die direkte Herkunft eines BSD-UNIX aus dem originalen UNIX und die für den Autor strukturierteren Entwicklungsmodelle sprechen für BSD-UNIX. Außerdem wird bei BSD-UNIX das mit dem Betriebssystem ausgelieferte Userland von den Distributionen betreut. Dies stellt auch die Qualität der grundlegenden Systemprogramme sicher. Aufgrund dieser kleinen Unterschiede fällt die Wahl auf BSD-UNIX.

Es gibt drei große BSD-Projekte: FreeBSD, NetBSD und OpenBSD. Jedes dieser Projekte hat verschiedene Ziele. Da FreeBSD sehr weit verbreitet ist, eine ausführliche Dokumentation und eine komfortable Installation bietet, soll für den Server FreeBSD als Betriebssystem genutzt werden.[4]

[4] Aufgrund fehlender Hardwareunterstützung musste bei der Umsetzung Linux genutzt werden.

3 Umsetzung

Dieses Kapitel beschreibt die praktische Umsetzung. Zu Beginn wird das zu erstellende System mit den geforderten Funktionen kurz aufgeführt. Anschließdend wird die Installation des Betriebssystems und die Konfiguration erklärt. Nachdem das System vollständig eingerichtet ist, wird untersucht ob die geforderten Ausfallszenarien eingehalten werden können.

3.1 Systembeschreibung

Um die Anforderung an die Speicherkapazität von mindesten 528GB zu erfüllen und ein RAID aufbauen zu können, werden neue Festplatten benötigt. Die auf dem Mainboard bereitgestellten ATA/IDE-Schnittstellen sind heute nur noch wenig verbreitet und wurden von dem neuen Standard „Serial ATA" (kurz: SATA) abgelöst. Deswegen wurde für den Server die folgende Hardware erworben:

- PCI PROMISE SATA300 TX2plus 2 Channel
- 3.5" Samsung 1000 GB SpinPoint F3 HD103SJ
- 3.5" HITACHI 1000 GB HDS721010CLA332

Durch den SATA-Controller von Promise können aktuelle Festplatten mit einer SATA-Schnittstelle verwendet werden. In einem RAID Level 1 bieten die zwei Festplatten mit 1TB genügend Speicherkapazität. Um die Wahrscheinlichkeit eines Ausfalls beider Festplatten in einem sehr kurzen Zeitraum zu minimieren, z.B. durch Fehler in einer Fertigungsreihe, wurden zwei Festplatten von unterschiedlichen Herstellern verwendet.

Nach einem Installationsversuch von FreeBSD und der zu späten Einsicht in die Hardwarekompatibilitätsliste wurde festgestellt, dass dieses keine Treiber für den SATA-Controller besitzt. Da bei der Auswahl des Controllers darauf geachtet wurde, dass Linux-Treiber verfügbar sind, kann statt FreeBSD ein Linux verwendet werden. Dies stellt wie in Kapitel 2.6.3 beschrieben keine Einschränkung dar, weil alle geforderten Funktionen von beiden Betriebssystemen erfüllt werden. Als Linux-Distribution wird Ubuntu Server Edition 10.04 LTS verwendet, da dies durch den Long Time Support (LTS) bis April 2015 unterstützt wird und zusammen mit der Desktop Edition sehr weit verbreitet ist [Dis].

Zugriff auf die Freigaben sollen nur Benutzer haben, welche Mitglied der Gruppe „backup" sind. Jeder Benutzer hat einen eigenen Ordner in dieser Freigabe, auf den nur er Schreibzugriff besitzt. Auf alle anderen Ordner erhält der Benutzer nur über die Rechte der Gruppe Lesezugriff. Diese Rechte sollen auf Dateisystemebene und soweit möglich auch auf Freigabeebene definiert werden.

Zusammenfassend wird ein System mit diesen Merkmalen erstellt:

Prozessor AMD Athlon(tm) XP 1600+ (1400MHz)

Mainboard Gigabyte GA-7DXR

Hauptspeicher 768MB (200MHz) DDR-SDRAM

SATA-Controller PCI PROMISE SATA300 TX2plus 2 Channel

Festplatte Samsung 1000GB SpinPoint F3 HD103SJ, HITACHI 1000GB HDS721010CLA332

RAID Level 1 (Mirroring) für alle Partitionen

Grafikkarte Gainward Geforce 2 TI (64MB)

Netzwerkkarte D-Link DFE-530TX

Betriebssystem Ubuntu Server Edition 10.04 (32-bit)

Anwendungen SSH-Server, Samba-Server

3.2 Installation

1. Herunterladen des Installationsmediums als Image von `http://www.ubuntu.com/server/get-ubuntu/download` und Brennen auf eine CD.

2. Den Computer von dieser CD booten und im ersten Menü die Sprache *Deutsch* wählen. Anschließend mit *Ubuntu Server installieren* die Installation starten. Diese wird durch ein Text User Interface (kurz: TUI), wie in Abbildung 3.1 zu sehen, geführt.

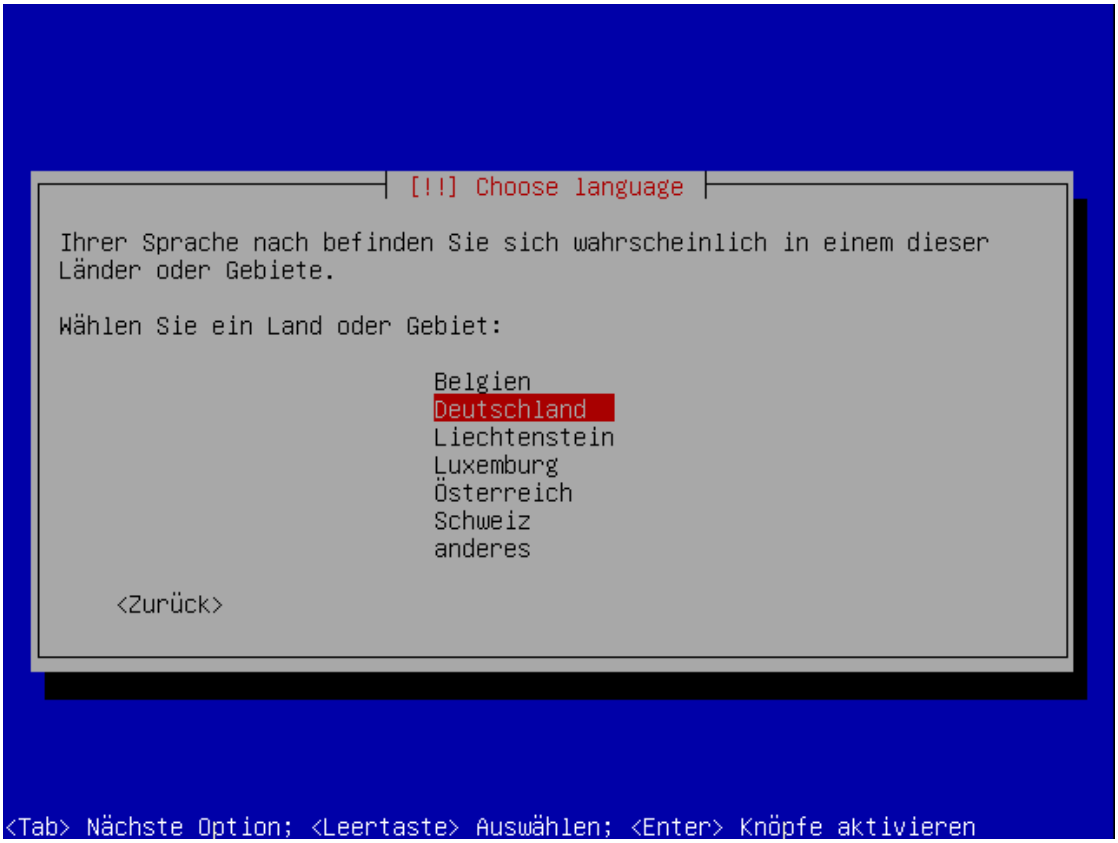

Abbildung 3.1: Text User Interface der Ubuntu Server Edition Installation.

3. In den nächsten Schritten werden das Land bzw. Gebiet und das Tastaturmodell gewählt.

4. Nun wird versucht die Netzwerkeinstellungen mit Hilfe eines DHCP-Server zu konfigurieren. Falls kein DHCP-Server vorhanden ist, können an dieser Stelle die Netzwerkeinstellungen manuell vorgenommen werden. In beiden Fällen muss nach der Konfiguration der Rechnername vergeben werden. Dieser Server erhält den Namen „backup".

5. Die Konfiguration der Zeitzone.

6. Im nächsten Schritt müssen die Festplatten konfiguriert werden. Dies kann *Geführt*, also automatisch, durchgeführt werden. Ein RAID-Verbund muss jedoch *Manuell* eingerichtet werden. Das Menü für die Partitionierung ist in Abbildung 3.2 abgebildet.

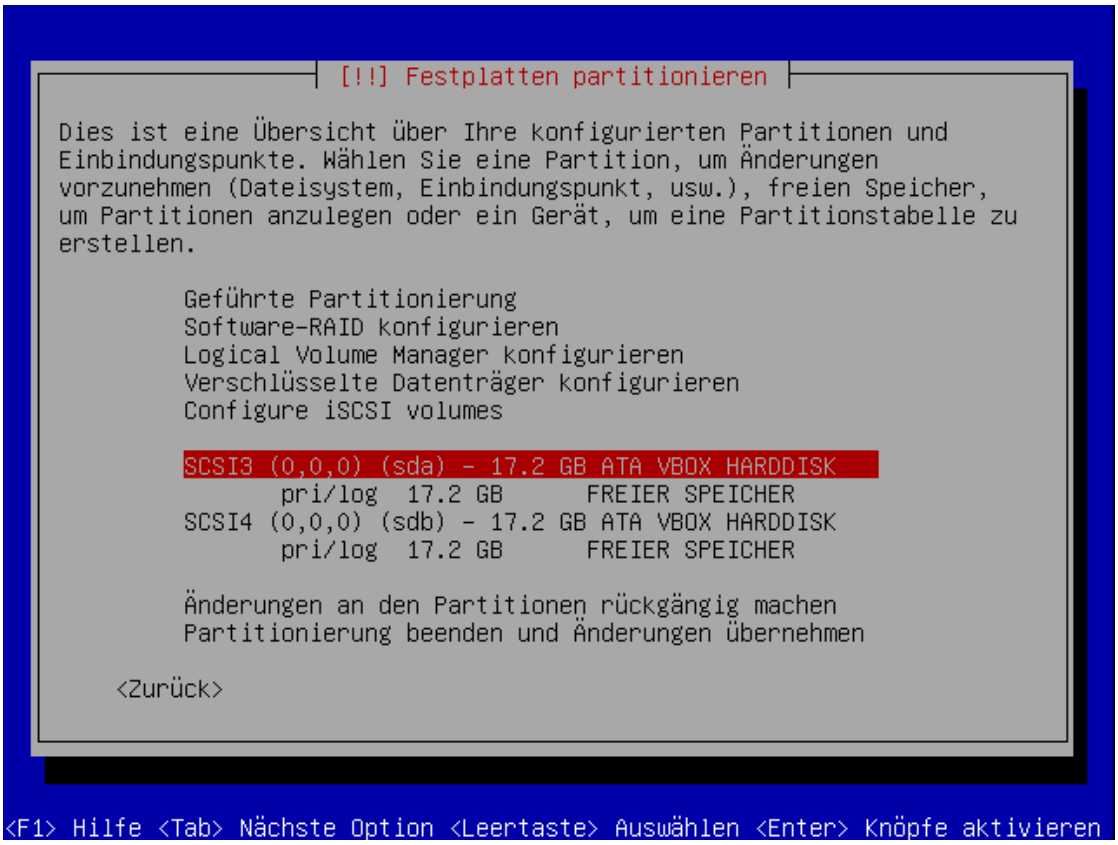

Abbildung 3.2: Menü zur Festplattenpartitionierung der Ubuntu Server Edition Installation.

An dieser Stelle sollen nur die Partitionen für das Betriebssystem eingerichtet werden. Zuerst müssen die Partitionen erstellt und für das RAID eingerichtet werden, um anschließend das RAID zusammenstellen zu können. Danach müssen die Partitionen formatiert und der Einhängepunkt festgelegt werden.

a) Partitionierung des Auslagerungsspeichers:
   i. *FREIER SPEICHER* von *SCSI1* auswählen und mit ENTER die Partitionierung starten.
   ii. Anschließend *Eine neue Partition erstellen* wählen.
   iii. *Neue Größe der Partition:* 2048 MB
   iv. *Typ der neuen Partition: Primär*
   v. *Position der neuen Partition: Anfang*
   vi. *Benutzen als: physikalisches Volume für RAID*
   vii. Mit *Anlegen der Partition beenden* den Vorgang beenden.
   viii. Diesen Vorgang für *SCSI2* wiederholen.

b) Partitionierung der Systempartition:

i. *FREIER SPEICHER* von *SCSI1* auswählen und mit ENTER die Partitionierung starten.
ii. Anschließend *Eine neue Partition erstellen* wählen.
iii. *Neue Größe der Partition:* 16384 MB
iv. *Typ der neuen Partition: Primär*
v. *Position der neuen Partition: Anfang*
vi. *Benutzen als: physikalisches Volume für RAID* setzen.
vii. *Boot-Flag: Ein* setzen.
viii. Mit *Anlegen der Partition beenden* den Vorgang beenden.
ix. Diesen Vorgang für *SCSI2* wiederholen.

c) Konfiguration des RAID:
i. *Software-RAID konfigurieren* wählen.
ii. *Änderungen auf das Speichergerät schreiben und RAID konfigurieren?* mit *Ja* bestätigen.
iii. *MD-Gerät erstellen* wählen.
iv. *Typ des Software-RAID-Geräts: RAID1*
v. *Anzahl der aktiven Geräte für das RAID1-Array* auf 2 setzen.
vi. *Anzahl der Reserve-Geräte für das RAID1-Array* auf 0 setzen.
vii. *Anzahl der aktiven Geräte für das RAID1-Array* auf `/dev/sda1` und `/dev/sdb1` setzen.
viii. Schritte für Systempartition mit `/dev/sda2` und `/dev/sdb2` wiederholen.
ix. Mit *Fertigstellen* den Vorgang beenden. Der Auslagerungspeicher ist nun auf `/dev/md0` und die Systempartition auf `/dev/md1` verfügbar.

d) Formatierung und Einhängepunkt konfigurieren:
i. *RAID1 Gerät #0, Nr. 1* wählen.
ii. *Benutzen als: Auslagerungsspeicher (Swap)*
iii. *Anlegen der Partition beenden* wählen.
iv. *RAID1 Gerät #1, Nr. 1* wählen.
v. *Benutzen als: Ext4 journaling file system*
vi. *Einhängepunkt (mount point): / - Das Wurzelsystem*
vii. *Anlegen der Partition beenden* wählen.

e) Mit *Partitionierung beenden und Änderungen übernehmen* die Änderungen übernehmen.

f) *Do you want to boot your system if your RAID becomes degraded?* mit *Ja* bestätigen, um das System nach einem Festplattenausfall mit der verbleibenden Festplatte zu booten.

g) *Änderungen auf die Festplatten schreiben?* mit *Ja* bestätigen.

7. Nun wird das Grundsystem installiert.

8. Anschließend wird die Konfiguration für den E-Mail-Server Postfix abgefragt. Da dieser nicht genutzt wird, kann *Keine Konfiguration* ausgewählt werden.

9. In diesem Schritt wird der Hauptbenutzer des Servers eingerichtet. Dieser besitzt die Berechtigung das System zu administrieren.

a) *Voller Name des neuen Benutzers:* Christof

b) *Benutzername für Ihr Konto:* christof

c) In den nächsten Schritten wird das Passwort angegeben und bestätigt.

d) *Ihren persönlichen Ordner verschlüsseln?* mit *Nein* ablehnen.

10. Der Paketmanager wird ohne die Angabe eines Proxy konfiguriert.

11. An dieser Stelle kann Software ausgewählt werden, welche zusätzlich zur Grundinstallation vorinstalliert werden soll.

    a) Bei *Wie möchten Sie Aktualisierungen auf diesem System verwalten?* wird *Keine automatischen Aktualisierungen* gewählt.

    b) In der Softwareauswahl werden *OpenSSH server* und *Samba file server* gewählt.

12. Im letzten Schritt der Installation wird der Bootloader `grub` eingerichtet.

    a) *GRUB-Bootloader in den Master Boot Record installieren?* mit *Nein* ablehnen, um sicherzustellen, dass der Bootloader in den Master Boot Record (kurz: MBR) beider Festplatten installiert wird.

    b) Bei *Device for boot loader installation* die Festplatten mit `/dev/sda` und `/dev/sdb` angeben.

13. Nach der Installation des Bootloaders ist die Installation beendet, die CD kann entfernt und der Server neugestartet werden.

14. Nach der Installation kann das System mit den folgenden Befehlen aktualisiert werden:

```
sudo apt-get update
sudo apt-get upgrade
sudo apt-get autoremove
```

3.3 Konfiguration des RAID

In diesen Kapitel wird die Konfiguration und die Administration eines RAID-Verbunds mit den Programmen `fdisk` und `mdadm` beschrieben.

3.3.1 Erstellung der Sicherungspartitionen

Bisher wurden nur die Systempartitionen und der Auslagerungsspeicher konfiguriert. Der restliche Speicherplatz von ungefähr 982GB soll für die Sicherung genutzt werden. Da die Synchronisation des RAID-Verbunds nach einem Ausfall nicht ohne Neubeginn unterbrochen werden kann, wird die verfügbare Speicherkapazität geteilt, sodass drei Partitionen von ungefähr 327GB entstehen. Messungen auf dem System ergaben eine Synchronisationsgeschwindigkeit von 55MB/s, somit würde eine Synchronisation einer Partition nicht länger als 100 Minuten dauern und die ersten Daten wären nach dieser Zeit bereits wieder dupliziert.

Nun wird die Partitionierung der Festplatten mit `fdisk` erklärt, um die Partitionen für die Erstellung der RAID-Verbünde vorzubereiten. Außerdem muss dieser Vorgang bei einem Ausfall einer Festplatte für die Ersatzfestplatte durchgeführt werden.

1. Start von `fdisk` für `/dev/sda`:

```
sudo fdisk /dev/sda
```

2. Befehlsliste von `fdisk` mit der Eingabe von *m* anzeigen lassen:

```
Befehl  Bedeutung
a (De)Aktivieren des bootfähig-Flags
b "bsd disklabel" bearbeiten
c (De)Aktivieren des DOS Kompatibilitätsflags
d Eine Partition löschen
l Die bekannten Dateisystemtypen anzeigen
m Dieses Menü anzeigen
n Eine neue Partition anlegen
o Eine neue leere DOS Partitionstabelle anlegen
p Die Partitionstabelle anzeigen
q Ende ohne Speichern der Änderungen
s Einen neuen leeren "Sun disklabel" anlegen
t Den Dateisystemtyp einer Partition ändern
u Die Einheit für die Anzeige/Eingabe ändern
v Die Partitionstabelle überprüfen
w Die Tabelle auf die Festplatte schreiben und das Programm ↩
   beenden
x Zusätzliche Funktionen (nur für Experten)
```

3. Die Partitionstabelle kann mit *p* angezeigt werden. Dies ist nützlich, wenn die Partitionen der aktiven Festplatte auf die neue Festplatte abgebildet werden sollen. Nach der zuvor beschriebenen Installation existiert diese Partitionstabelle:

```
Platte /dev/sda: 1000.2 GByte, 1000204886016 Byte
255 Köpfe, 63 Sektoren/Spur, 121601 Zylinder
Einheiten = Zylinder von 16065 x 512 = 8225280 Bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00013090

Gerät boot. Anfang  Ende  Blöcke  Id  System
/dev/sda1   1 249 1998848 fd  Linux raid autodetect
Partition 1 endet nicht an einer Zylindergrenze.
/dev/sda2 * 249 2241  16000000  fd  Linux raid autodetect
```

4. Um die verbleibende Kapazität verfügbar zu machen, muss zunächst eine *erweiterte Partition* erstellt werden.

   a) Eine neue Partition mit *n* anlegen.

   b) Im nächsten Schritt mit *e* eine *Erweiterte* Partition erstellen.

   c) Diese Partition erhält die *Partitionsnummer* 3, da 1 und 2 bereits verwendet werden.

   d) Der *Erste Zylinder* ist 2243.
   Bei der Partitionierung während der Installation wurden das Ende der ersten und der Anfang der zweiten Partition auf den selben Zylinder gesetzt. Dies ist in `fdisk` unzulässig. Daher wird der Anfang und das Ende der zweiten Partition hypothetisch um einen Zylinder verschoben, womit diese bei Zylinder 2242 endet und die nächste Partition bei dem Zylinder 2243 beginnen kann. Dadurch können Probleme beim manuellen Partitionieren einer neuen Festplatte verhindert werden.

   e) Der *Last Zylinder* ist 121592.
   Auch hier werden nicht alle 121601 Zylinder genutzt, um für zuvor beschriebene Probleme einen Puffer zu haben.

5. Die restlichen 119349 Zylinder können nun auf die drei Partitionen verteilt werden, welche als logische Partition eingerichtet werden.
   a) Eine neue Partition mit *n* anlegen.
   b) Im nächsten Schritt mit *1* eine *Logische Partition* erstellen.
   c) Der *Erster Zylinder* ist 2243.
   d) Der *Last Zylinder* ist 42025.
   e) Diese Schritte für die restlichen zwei Partitionen wiederholen (42026, 81808; 81809, 121592).
6. Für die logischen Partitionen muss noch der Dateisystemtyp geändert werden.
   a) Den Dateisystemtyp einer Partition mit *t* ändern.
   b) *Partitionsnummer* der logischen Partitonen wählen z.B. 5.
   c) *Hex code* für *Linux raid autodetect* ist *fd*.
   d) Diese Schritte für 6 und 7 wiederholen.
7. Nun können die vorgenommenen Einstellung mit *p* kontrolliert werden:

```
Gerät boot. Anfang  Ende  Blöcke  Id  System
/dev/sda1   1 249 1998848 fd  Linux raid autodetect
Partition 1 endet nicht an einer Zylindergrenze.
/dev/sda2 * 249 2241  16000000  fd  Linux raid autodetect
/dev/sda3   2243  121592  958678875 5 Erweiterte
/dev/sda5   2243  42025 319556916 fd  Linux raid autodetect
/dev/sda6   42026 81808 319556916 fd  Linux raid autodetect
/dev/sda7   81809 121592  319564948+  fd  Linux raid ↩
   autodetect
```

8. Einstellungen mit *w* speichern und das Programm beenden.
9. Diese Schritte für `/dev/sdb` wiederholen.
10. Computer gegebenenfalls neustarten.

Nach diesen Schritten sind die Partitionen für den RAID-Verbund vorbereitet und können zu einem RAID Level 1 verbunden werden.

1. Partitionen zu RAID Level 1 zusammenstellen:

```
sudo mdadm --create --verbose /dev/md2 --auto=yes --level=1 ↩
   --raid-devices=2 /dev/sda5 /dev/sdb5
sudo mdadm --create --verbose /dev/md3 --auto=yes --level=1 ↩
   --raid-devices=2 /dev/sda6 /dev/sdb6
sudo mdadm --create --verbose /dev/md4 --auto=yes --level=1 ↩
   --raid-devices=2 /dev/sda7 /dev/sdb7
```

2. Die entstandenen RAID-Verbünde im Dateisystem „ext4" formatieren:

```
sudo mkfs.ext4 /dev/md2
sudo mkfs.ext4 /dev/md3
sudo mkfs.ext4 /dev/md4
```

3. Die neuen RAID-Verbünde müssen noch in `/etc/mdadm/mdadm.conf` eingetragen werden:
   a) RAID-Informationen abfragen:

```
sudo mdadm --detail --scan
```

b) Ergebnis mit allen RAID-Verbünden:

```
ARRAY /dev/md0 level=raid1 num-devices=2 metadata=00.90 ↩
   UUID=1828dabb:a0dbf7f9:0a5f13b6:fb892ba6
ARRAY /dev/md1 level=raid1 num-devices=2 metadata=00.90 ↩
   UUID=674e08d3:adfb6a45:c3c2489d:e2b9824f
ARRAY /dev/md2 level=raid1 num-devices=2 metadata=00.90 ↩
   UUID=78a8a583:272b9b61:c91d1289:ceb97d9c
ARRAY /dev/md3 level=raid1 num-devices=2 metadata=00.90 ↩
   UUID=bb57c2d7:c33dd952:c91d1289:ceb97d9c
ARRAY /dev/md4 level=raid1 num-devices=2 metadata=00.90 ↩
   UUID=50713bca:dffb23e6:c91d1289:ceb97d9c
```

c) `metadata=00.90` zu `metadata=0.90` ändern und neue Verbünde in `/etc/mdadm/mdadm.conf` eintragen.

4. Die RAID-Verbünde der Sicherungspartitionen sind nun fertig eingerichtet und werden synchronisiert. Der Status kann mit den folgenden Befehlen abgefragt werden:

```
watch -n1 cat /proc/mdstat
sudo mdadm --detail /dev/md<number>
```

3.3.2 „Degraded RAID" Wiederherstellen

Als „degraded" wird der Status eines RAID-Verbunds bezeichnet, wenn die Redundanz aufgrund eines Ausfalls einer Festplatte nicht mehr vorhanden ist. Während diesen Status sind die Daten im vorliegenden System nur noch auf einer Festplatte vorhanden und ein Ausfall dieser würde einen Datenverlust nach sich ziehen. Deswegen ist es wichtig ein „degraded" RAID so schnell wie möglich wiederherzustellen. Folgende Befehle werden dazu benötigt:

- Partition von einem RAID-Verbund als fehlerhaft markieren:

```
sudo mdadm <raid array> --set-faulty <partition>
```

- Partition aus einem RAID-Verbund entfernen:

```
sudo mdadm <raid array> --remove <partition>
```

- Partition zu einem RAID-Verbund hinzufügen:

```
sudo mdadm <raid array> --add <partition>
```

Am Beispiel der Systempartition und dem Ausfall der Festplatte `/dev/sda` wird das Wiederherstellen schrittweise beschrieben:

1. Zuerst muss die Partition aus dem RAID-Verbund entfernt werden:

```
sudo mdadm /dev/md1 --remove /dev/sda1
```

Falls die Partition noch in Benutzung ist, muss sie zuvor als fehlerhaft markiert werden:

```
sudo mdadm /dev/md1 --set-faulty /dev/sda1
```

2. Nun muss die neue Festplatte partitioniert werden. Dies ist in Kapitel 3.3.1 beschrieben.

3. Nachdem die Partition erstellt wurde, kann sie dem RAID-Verbund hinzugefügt werden:

```
sudo mdadm /dev/md1 --add /dev/sda1
```

4. Anschließend sollten die Einträge in `/etc/mdadm/mdadm.conf` mit der Ausgabe des folgenden Befehls verglichen und ggf. korrigiert werden:

```
sudo mdadm --detail --scan
```

5. Um von der neuen Festplatte bei einem Ausfall der alten booten zu können, muss auf dieser der Bootloader in den MBR installiert werden:

```
sudo grub-install /dev/sda
```

   Zusätzlich muss das *bootfähig-Flag* der Systempartition aktiviert werden.

3.4 Setzen der Einhängepunkte

Um auf die Daten der RAID-Verbünde zugreifen zu können, müssen diese erst an einem Einhängepunkt eingebunden werden. Unter Ubuntu werden Laufwerke unter `/media` eingebunden. In diesem Ordner werden zunächst die Ordner `backup1`, `backup2` und `backup3` erstellt:

```
sudo mkdir /media/backup1
sudo mkdir /media/backup2
sudo mkdir /media/backup3
```

Anschließend können diese Einhängepunkte persistent in `/etc/fstab` eingetragen werden, um diese nach jedem Neustart beizubehalten:

```
/dev/md2  /media/backup1  ext4  defaults  0 0
/dev/md3  /media/backup2  ext4  defaults  0 0
/dev/md4  /media/backup3  ext4  defaults  0 0
```

3.5 Erstellung der Benutzer, Gruppen und Zugriffsrechte

Der Zugriff auf Dateisystemebene wird durch Benutzer und Gruppen organisiert. Hierbei wird jeder Datei und jedem Ordner ein Eigentümer und eine Gruppe zugewiesen. Weiterhin werden dem Eigentümer, der Gruppe und allen Anderen, welche nicht Eigentümer oder Mitglied der Gruppe sind, Zugriffsrechte zugewiesen. Die Tabelle 3.1 listet die verfügbaren Zugriffsrechte in der Oktalnotation und der symbolischen Notation auf. Bei

Zugriffsrechte	Oktalnotation	Symbolische Notation
Ausführen	1	x
Schreiben	2	w
Lesen	4	r

Tabelle 3.1: Auflistung der Zugriffsrechte und deren Notation.

Verwendung der Oktalnotation werden die Werte der gewünschten Zugriffsrechte addiert. Allgemein gilt, es ist alles verboten, was nicht explizit erlaubt ist.

Mit den folgenden Befehlen können die Zugriffsrechte modifiziert werden:

- Eigentümer für einen Ordner oder einer Datei setzen:

```
sudo chown [-R] <user> <file | directory>
```

- Gruppe für einen Ordner oder einer Datei setzen:

```
sudo chgrp [-R] <group> <file | directory>
```

- Zugriffsrechte für einen Ordner oder einer Datei setzen (Oktalnotation):

```
sudo chmod [-R] <owner><group><other> <file | directory>
```

- Bei Verwendung der Option `-R` werden die Änderungen auch für alle Unterordner und darin befindlichen Dateien übernommen.

Außerdem müssen auch Benutzer und Gruppen verwaltet werden. Hierfür stehen diese Befehle zur Verfügung:

- Benutzer erstellen:

```
sudo adduser <username>
```

- Benutzer löschen:

```
sudo deluser <username>
```

- Grupper erstellen:

```
sudo addgroup <groupname>
```

- Grupper löschen:

```
sudo delgroup <groupname>
```

- Benutzer einer Gruppe hinzufügen:

```
sudo adduser <username> <groupname>
```

- Benutzer aus einer Gruppe entfernen:

```
sudo deluser <username> <groupname>
```

Auf dem Backup-Server sollen alle Mitglieder der Gruppe „backup" Lese- und Ausführungsrechte auf den Sicherungspartitionen haben. Jeder Benutzer erhält einen eigenen Ordner, für den er Eigentümer ist und somit alle Zugriffsrechte besitzt. Andere Benutzer haben nur Lesezugriff auf diese Daten. Außerdem sollen alle neuen Ordner und Dateien die Gruppe sowie die Rechte erben. Um den Server administrieren zu können, muss ein Benutzer Mitglied der Gruppe „admin" sein. Diese Anforderungen werden mit den folgenden Befehlen eingerichtet:

- Benutzer „volker" erstellen:

```
sudo adduser volker
```

- Benutzer „volker" der Gruppe „admin" hinzufügen:

```
sudo adduser volker admin
```

- Gruppe „backup" erstellen:

```
sudo addgroup backup
```

- Benutzer „volker" der Gruppe „backup" hinzufügen:

```
sudo adduser volker backup
```

- Den Ordnern `backup1`, `backup2` und `backup3` die Gruppe „backup" zuweisen:

```
sudo chgrp -R backup /media/backup1
sudo chgrp -R backup /media/backup2
sudo chgrp -R backup /media/backup3
```

- Setzen der Zugriffsrechte:

```
sudo chmod -R 754 /media/backup1
sudo chmod -R 754 /media/backup2
sudo chmod -R 754 /media/backup3
```

- Setzen der erweiterten Zugriffsrechte, damit alle neuen Daten die Gruppe erben:

```
sudo chmod -R g+s /media/backup1
sudo chmod -R g+s /media/backup2
sudo chmod -R g+s /media/backup3
```

- Setzen der `umask` in jedem der Ordner `backup1`, `backup2` und `backup3`, damit die Zugriffsrechte für neue Daten richtig gesetzt werden:

```
umask 0023
```

  Im Gegensatz zu dem Befehl `chmod` werden hier alle Zugriffsrechte angegeben, die ausgeschlossen werden sollen!

Nachdem die Zugriffrechte für die Sicherungspartitionen gesetzt sind, können die Ordner für die Benutzer eingerichtet werden:

- Erstellen der Ordner für den Benutzer „volker":

```
sudo mkdir /media/backup1/volker
sudo mkdir /media/backup2/volker
sudo mkdir /media/backup3/volker
```

- Setzen der Gruppe „backup" und „volker" als Eigentümer:

```
sudo chown -R volker:backup /media/backup1/volker
sudo chown -R volker:backup /media/backup2/volker
sudo chown -R volker:backup /media/backup3/volker
```

3.6 Netzwerkeinstellungen

Während der Installation wurden die Netzwerkeinstellungen automatisch durch einen DHCP-Server bezogen. Diese können manuell in `/etc/network/interfaces` konfiguriert werden:

- Setzen von statischen Adressen für den Netzwerkadapter `eth0`:

```
auto eth0
iface eth0 inet static
  address <ip address>
  netmask <subnet mask>
  gateway <gateway>
  dns-nameservers <dns server 1> <dns server 2>
```

- Einstellungen für den Netzwerkadapter `eth0` von einem DHCP-Server beziehen:

```
auto eth0
iface eth0 inet dhcp
```

- Neustart der Netzwerkadapter:

```
sudo /etc/init.d/networking restart
```

3.7 Konfiguration von Samba

Der Samba-Server ermöglicht die Freigabe von Daten über das SMB-Protokoll. Für alle Freigaben können zusätzlich Zugriffsrechte durch den Samba-Server definiert werden. Diese können jedoch nur die Rechte auf Dateisystemebene weiter einschränken, aber nicht erweitern! Dies ermöglicht es die Zugriffsrechte nicht zweimal definieren zu müssen, da der Samba-Server die Zugriffsrechte auf Dateisystemebene nicht umgehen kann. Trotzdem soll der Samba-Server nur Mitgliedern der Gruppe „backup" Zugriff auf die Freigaben gewähren.

Hierfür müssen das Security Level auf „user" gesetzt und die Freigaben der drei Sicherungspartitionen konfiguriert werden. Die Einstellungen für den Samba-Server müssen in `/etc/samba/smb.conf` vorgenommen werden.

- Arbeitsgruppennamen setzen:

```
workgroup = SERVER
```

- Security Level setzen:

```
security = user
```

- Passwortverschlüsselung aktivieren:

```
encrypt passwords = true
```

- Der Abgleich zwischen den Samba-Benutzern und den Systembenutzern wird durch das vorinstallierte Paket `libpam-smbpass` und den dazugehörigen Einträgen gewährleistet.

- Die Freigabe für den Ordner `/media/backup1` mit dem Namen `backup1` wird durch folgende Einträge konfiguriert:

```
[backup1]
  comment = First backup folder
  path = /media/backup1
  browsable = yes
  guest ok = no
  read only = yes
  create mask = 0754
  valid users = @backup
  write list = @backup
```

comment Beschreibung und weitere Information über die Freigabe.

path Der Ordner `/media/backup1` wird freigegeben.

browsable Die Freigabe wird angezeigt und aufgelistet.

guest ok Der Gastzugriff ist nicht erlaubt.

read only Es ist nur der Lesezugriff möglich, wenn nicht anders festgelegt.

create mask Festlegung der Zugriffsrechte für erstellte Daten.

valid users Nur die Mitglieder der Gruppe „backup" haben Zugriff.

write list Nur die Mitglieder der Gruppe „backup" haben Schreibzugriff.

- Die Freigaben für die Ordner `backup2` und `backup3` können analog zu `backup1` erstellt werden.
- Die `/etc/samba/smb.conf` kann mit den folgenden Befehl überprüft und ohne Kommentare angezeigt werden:

```
testparm /etc/samba/smb.conf
```

- Samba-Server neustarten, um die Einstellungen zu übernehmen:

```
sudo restart smbd
sudo restart nmbd
```

3.8 Untersuchung der Ausfallszenarien

Für den Server wurden drei Ausfallszenarien definiert, bei denen keine Daten verloren gehen dürfen:

1. Ausfall des Speichercontrollers und/oder
2. einer Festplatte und/oder
3. anderer Komponenten.

3.8.1 Ausfall des Speichercontrollers

Wenn der Speichercontroller defekt ist, müssen die Daten auf den Festplatten an einem anderen Controller ausgelesen werden können, insofern der Ausfall die Festplatten nicht beschädigt hat.

Da Windows das Dateisystem „ext4" von Linux nicht unterstützt, können die Daten mit Hilfe einer Linux-Live-Distribution ausgelesen werden. In einem Terminal können mit dem Befehl

```
sudo fdisk -l
```

angeschlossene Geräte aufgelistet werden. In dieser Liste sind die Partitionen der angeschlossenen Festplatte aufgeführt. Angenommen die Festplatte ist am ersten SATA-Controller angeschlossen, so sind dies `/dev/sda1`, `/dev/sda2`, `/dev/sda3`, `/dev/sda5`, `/dev/sda6` und `/dev/sda7`. Auf den Partitionen 5 bis 7 befinden sich die relevanten Daten, welche ausgelesen werden sollen. Um die Partition `/dev/sda5` zu lesen, muss zuerst ein Einhängepunkt erstellt und die Partition anschließend unter diesen eingehangen werden:

```
sudo mkdir /media/backup1
sudo mount -t ext4 --read-only /dev/sda5 /media/backup1
```

Nun können die Daten von `/media/backup1` gelesen und auf beliebige andere Datenträger kopiert werden.

Dieses Vorgehen wurde erfolgreich an einen Computer mit dem Mainboard MA790XT-UD4P von Gigabyte und der Linux-Live-Distribution KNOPPIX 6.4.3 untersucht. Falls das Laufwerk nach dem Auslesen für die Wiederherstellung eines RAID genutzt werden soll, muss es im Lesezugriff eingehangen werden, sonst kann dieser Vorgang nicht fehlerfrei durchgeführt werden. Bei einem Test, in dem jeweils eine Datei gelöscht, hinzugefügt und modifiziert wurden, schlug das Einhängen mit einem Kernel-Absturz fehl.

3.8.2 Ausfall einer Festplatte

Der Ausfall einer Festplatte führt aufgrund des RAID Level 1 zu keinem Datenverlust, da die Daten weiterhin auf einer zweiten Festplatte vorhanden sind. Wenn eine Partition oder Festplatte ausfällt, erhält dieser RAID-Verbund den Status „degraded". In diesem Fall sollte die defekte Festplatte schnellst möglich ausgetauscht werden und anschließend der RAID-Verbund, wie in Kapitel 3.3.2 beschrieben, wiederhergestellt werden. Bei diesem Vorgang werden alle betroffenen RAID-Verbünde synchronisiert. Nur wenn diese Synchronisation vollständig abgeschlossen wurde, sind alle Daten auf der neue Festplatte oder Partition vorhanden.

Dieses Szenario wurde untersucht, indem eine der beiden Festplatten aus dem Server entfernt wurde. Bei dieser Festplatte wurde die Partitionstabelle gelöscht und anschließend wieder in den Server eingebaut. Das System erkannte alle RAID-Verbünde als „degraded" und startete erfolgreich. Nun konnten alle RAID-Verbünde, wie in Kapitel 3.3.2 beschrieben, wiederhergestellt werden.

3.8.3 Ausfall anderer Komponenten

Da die erfolgreiche Wiederherstellung der Daten in den beiden vorherigen Szenarien gezeigt werden konnte, können die Daten auch bei einem Ausfall anderer Komponenten gelesen werden, insofern mindestens eine Festplatte nicht beschädigt wird.

Erwähnenswert ist der Ausfall des Netzteils oder andere Störungen im Stromnetz. Hierbei werden oft weitere Geräte in Mitleidenschaft gezogen. Gegen Störungen im Stromnetz können Netzteile mit Schutzvorkehrungen wie Über- & Unterspannungsschutz, Schutz vor Stromspitzen u.m., sowie das physische Trennen vom Netz helfen.

Bei dem Ausfall eines Netzteils kann kaum vorhergesagt werden, ob und wie stark andere Komponenten beschädigt werden. Ähnlich wie bei einem Brand, Wasserschaden oder Diebstahl kann hier nur durch eine weitere Kopie an einem physisch entfernten Ort ein Datenverlust vorgebeugt werden.

4 Schlusswort

4.1 Zusammenfassung

Ein Backup-System kann auf verschiedene Weisen umgesetzt werden. Für das vorliegende Szenario wurden die Möglichkeiten eines NAS und eines Servers genauer untersucht. Obwohl die Grundkonfiguration eines NAS einfacher und der Stromverbrauch niedriger als bei einem Server ist, wurde das System als Server mit bereits vorhandener PC-Hardware erstellt. Dies ermöglicht das System um beliebige weitere Dienste zu erweitern und stellt die Datenrettung bei verschiedenen Ausfallszenarien sicher.

Um bei dem Ausfall einer Festplatte oder eines SATA-Controllers die Datensicherheit gewährleisten zu können, wurden die RAID Level 0, 1 und 5 untersucht. Nur die RAID Level 1 und 5 bieten eine Redundanz und stellen somit die Datensicherheit bei einem Festplattenausfall sicher. Die Datensicherheit bei Ausfall des SATA- oder RAID-Controllers ist von dem verwendeten RAID Level und dem Controller abhängig. Da beim RAID Level 5 die Daten über mehrere Laufwerke verteilt sind, können die Daten nicht von einem einzelnen Laufwerk rekonstruiert werden. Dies ist nur beim RAID Level 1 möglich, weil die Daten auf allen Laufwerken gespiegelt sind und ein einzelnes Laufwerk alle nötigen Informationen zur Rekonstruktion enthält. Zusätzlich ist bei einem Hardware-RAID aufgrund proprietärer Implementierungen nicht gewährleistet, dass die Daten an jedem beliebigen Controller ausgelesen werden können. Aufgrund dieser Überlegungen wurde ein Software-RAID mit dem Level 1 verwendet.

Zum Sichern und Lesen der Daten muss die Speicherkapazität in einem 100-Mbit/s-Ethernet freigegeben werden. Hierzu wurden die Protokolle FTP, SSH und SMB in Hinblick auf die Sicherheit und die Einbindung in ein Windows-Netzwerk untersucht. FTP ist ungeeignet, da es keine sichere Authentifizierung bereitstellt. SSH bietet eine vollständig verschlüsselte Authentifizierung sowie Datenübertragung und einen Zugriff auf die Kommandozeile. Dadurch eignet sich SSH für die sichere Datenfreigabe und den entfernten Zugriff über das Internet. SMB stellt nur eine verschlüsselte Authentifizierung zur Verfügung. Die Datenübertragung findet unverschlüsselt statt. Aufgrund der Integration in ein Windows-Netzwerk ohne den Einsatz von Zusatzanwendungen wird es für die Freigabe in einem lokalen Netzwerk genutzt.

Vor der praktischen Umsetzung muss noch ein geeignetes Betriebssystem ausgewählt werden. Zum Vergleich wurden hierzu je ein Repräsentant für Windows, BSD-UNIX und Linux gewählt. Windows Server 2008 ist aufgrund der höchsten Hardwareanforderung und der unzureichenden Administration über die Kommandozeile nur schlecht für den Server geeignet. Ähnliche Hardwareanforderungen sowie gleiche Funktionen bieten Ubuntu Server Edition 10.04 und FreeBSD 8.1. Aufgrund des direkten Ursprungs aus UNIX sollte FreeBSD genutzt werden, jedoch war dies durch fehlende Treiber nicht möglich. Stattdessen wurde die Linux-Distribution Ubuntu Server Edition 10.04 gewählt.

Nach dieser Vorbetrachtung besteht das umzusetzende System aus einem Server mit dem Betriebssystem Ubuntu Server Edition 10.04. Die System- sowie die Sicherungspartitionen sind zu mehreren RAID Level 1 verbunden.

Die Installation und die Einrichtung der RAID-Verbünde für die System- und Auslagerungspartition ist durch das TUI auch für Anfänger möglich. Die Einrichtung und Verwaltung der RAID-Verbünde wird mit den Anwendungen `fdisk` und `mdadm` durchgeführt. Die Partitionierung der Laufwerke erfolgt mit `fdisk`. Anschließend kann ein RAID mit `mdadm` und den Argumenten `--create`, `--add` und `--remove` erstellt bzw. konfiguriert

werden.

Das Rechtemanagement wird über Benutzer und Gruppen geregelt. Alle Ordner und Dateien können Ausführ-, Lese- und Schreibrechte für ihren Eigentümer, Mitglieder einer Gruppe und Fremden zugewiesen bekommen. Benutzer und Gruppen können mit `adduser`, `deluser`, `addgroup` und `delgroup` erstellt bzw. gelöscht werden. Die Zuweisung von Eigentümern, Gruppen und Rechten erfolgt mit den Befehlen `chown`, `chgrp` und `chmod`.

Mit Hilfe von Samba werden die Sicherungspartitionen über das SMB-Protokoll freigegeben. Hierfür muss die Konfigurationsdatei `/etc/samba/smb.conf` angepasst werden. Das Security Level „user" mit der Verwendung des Pakets `libpam-smbpass` ermöglicht die Nutzung der Systembenutzer. Die wichtigsten Parameter einer restriktiven Samba-Freigabe sind `path`, `read only`, `valid users` und `write list`.

Die Datensicherheit bei dem Ausfall des Speichercontrollers, einer Festplatte und andere Komponenten wurde praktisch untersucht. Nach einem simulierten Ausfall des Controllers konnten alle Partitionen erfolgreich an dem Mainboard MA790XT-UD4P von Gigabyte ausgelesen werden. Anschließend wurde durch das Löschen der Partitionstabelle ein Festplattendefekt vorgetäuscht. Das System startete erfolgreich im RAID-Status „degraded". Nachdem die Festplatte neu partitioniert war, konnte das RAID erfolgreich wiederhergestellt werden. Da die Festplatten an anderen Controllern ausgelesen werden können, ist die Datensicherheit durch den Ausfall anderer Komponenten nicht gefährdet, solange mindestens eine Festplatte unbeschädigt ist. Besonders bei Störung in der Stromversorgung werden nicht selten auch andere Komponenten beschädigt. Zur Sicherheit gegen solche Störungen hilft nur eine zweite physikalische Kopie.

4.2 Ausblick

Der Backup-Server für sich allein ist nur ein Bestandteil eines Sicherungskonzepts. So sind auch die genutzten Dateiformate ein wichtiger Punkt für ein erfolgreiches Konzept. Da für viele Programme und die damit verbundenen Dateiformate die Unterstützung und Weiterentwicklung genauso schnell eingestellt wird, wie sie populär geworden sind, eignet sich nicht jedes Format für die Archivierung. Die Nutzung von standardisierten oder „human-readable"[1] Dateiformaten stellt sicher, dass Dateien auch noch nach mehr als zehn Jahren lesbar sind.

Des Weiteren sollte auch immer eine zweite physikalische Kopie genutzt werden, da zum Beispiel ein defektes Netzteil oder Störungen im Stomnetz die Festplatten beschädigen können, womit alle Daten auf diesem System verloren sind. Wenn möglich, sollte diese Kopie an einem anderen Ort aufbewahrt werden, um auch gegen höhere Gewalt abgesichert zu sein.

Bei der Verwendung von mehreren Backup-Systemen besteht grundätzlich die Frage, wie die Daten auf die Systeme verteilt bzw. synchronisiert werden. So können die Daten manuell auf jeden Server kopiert werden oder der Anwender kopiert die zu sichernden Daten auf ein Backup-System, welches diese selbständig auf die anderen Systeme verteilt. Hierzu kann zum Beispiel die Anwendung `rsync` verwendet werden.

Die manuelle Sicherung jeden Monat kann ebenfalls automatisiert werden. So könnte täglich ein automatisierter Backup-Vorgang eingerichtet werden, der die Daten von allen Clients auf ein Backup-System sichert. Dies würde den Aufwand und den Zeitraum zwischen zwei Sicherungen verringern.

Darüber hinaus kann das System auch neben den Backup-Diensten weitere Dienste bereitstellen. Ein DHCP- und WINS-Server können zur Unterstützung der Netzwerkverwaltung betrieben werden. Außerdem ist eine Benutzerdatenbank für eine zentrale Verwaltung aller Benutzer und deren Authentifizierung denkbar.

[1] deutsch: vom Menschen lesbar

Literaturverzeichnis

[BS00] Bruce, Bob ; Stokely, Murray: *FreeBSD vs. Linux vs. Windows 2000*, 2000. http://www.freebsd.org/marketing/os-comparison.html

[BSD] *The BSDstats Project.* Website. http://www.bsdstats.org. – Abgerufen: 06.01.2011

[Dis] *DistroWatch.com.* Website. http://distrowatch.com. – Abgerufen: 06.01.2011

[Han05] Handwerkskammer Halle (Saale) (Hrsg.): *Sachverständigenordnung - Gesetzliche Regelungen.* Handwerkskammer Halle (Saale), November 2005

[Mic10] Microsoft (Hrsg.): *Microsoft SMB Protocol Authentication.* Microsoft, Dezember 2010. http://msdn.microsoft.com/en-us/library/aa365234%28v=vs.85%29.aspx. – Abgerufen: 13.01.2011

[Net] Netgear (Hrsg.): *Netgear: ReadyNAS Duo - Datenblatt.* Netgear, http://www.netgear.de/Produkte/Netzwerkspeicher/ReadyNASDuo/datenblatt.html. – Abgerufen: 10.01.2011

[PR83] Postel, J. ; Reynolds, J.: *RFC854 - Telnet Protocol*, Mai 1983

[PR85] Postel, J. ; Reynolds, J.: *RFC959 - File Transfer Protocol*, Oktober 1985

[Tan02] Tanenbaum, Andrew S.: *Moderne Betriebssysteme.* 2. Pearson Studium, 2002

[Tan06] Tanenbaum, Andrew S.: *Computerarchitektur.* 5. Pearson Studium, 2006

Abbildungsverzeichnis

Abkürzungsverzeichnis

FTP File Transfer Protocol

MBR Master Boot Record

MTBF Mean-Time-Between-Failure

NAS Network Attached Storage

RAID Redundant Array of Independent Disks

SATA Serial ATA

SFTP SSH File Transfer Protocol

SMB Server-Message-Block-Protokoll

SSH Secure Shell

TUI Text User Interface