Sauver les CD
Anforderungsspezifikation "Speicherbox im Archiv"

Inhalt

1 Projektbeschreibung

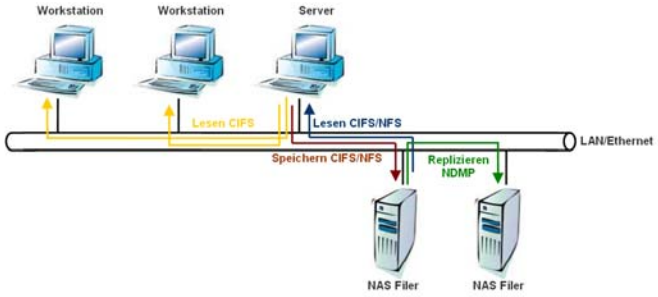
1.1 Ausgangslage

Grössere Datenmengen aus Digitalisierungsprojekten und von CD/DVD-Sammlungen sollen im Archiv preisgünstig gespeichert werden. Erwartet werden *Archivtauglichkeit* bezüglich Sicherheit, einfache Administration und ein Preis nicht über 10'000 sfr.[1]. Die Lösung soll die Datenspeicherung *(Bitstream Preservation)* von bis zu 4 TB für drei Jahre gewährleisten.

1.2 Konzept

Die Lösung soll aus zwei oder drei NAS Speicherboxen[2] mit je 3-4 TB Speicherplatz (netto) bestehen. Die Boxen werden ins Intranet des Archivs integriert. Die Zugriffsberechtigung[3] soll den Zugriff auf den Speicherplatz auf einen (oder ausgewählte) Rechner im Archiv begrenzen. Von diesem Rechner aus sollen Speichern und Lesen der Daten vorgenommen werden.

Die eingesetzte *Storage Management Software* soll den Inhalt der einen Box automatisch auf die zweite Box spiegeln (WORM[4] Mode). Zudem soll ein periodischer Integritätscheck die Lesbarkeit und die Unveränderheit der Daten sicherstellen.



Aufbau der Speicherboxlösung

2 Anforderungen

2.1 Anforderungen NAS Hardware

a) Die Speicherboxen sollen aus Gründen von Platzbedarf, Stromverbrauch und Lautstärke als ***Kompaktsystem*** realisiert sein. Sie sollen eine geringe Stromaufnahme und Geräuschentwicklung aufweisen, sodass sie ohne spezielle Raumanforderungen betrieben werden können.

b) Die Datenübertragung soll über ***Ethernet*** stattfinden, eine Gigabit-Ethernetschnittstelle ist nicht unbedingt erforderlich.

c) Als dateibasierender Dienst, über den der Massenspeicher im Netzwerk zugreifbar wird, muss ***SMB/CIFS***[5] angeboten werden, NFS[6] ist optional.

d) Die Daten- und Ausfallsicherheit muss mit mindestens ***RAID Level*** 5, besser aber RAID 6[7] installiert werden können. Ob die RAID Festplattenorganisation hardware- oder softwareseitig implementiert wird, ist nebensächlich.

---

[1] Im KOST-Projekt ***arcun*** wurde für *full service bitstream preservation* ein Preis von 4500.- sfr./TB/Jahr ermittelt. Hardwarekosten sind nach einem verlässlichen Schätzwert etwa 1/4 der Gesamtkosten. Bei drei Terabyte und drei Jahren Laufzeit kommen wir auf Hardwarekosten von etwa 10'000.- sfr.

[2] NAS, *Network-Attached Storage*, bezeichnet einfach zu verwaltende Dateiserver *(Filer)*, auf die von anderen Computern über ein lokales Netzwerk zugegriffen werden kann.

[3] Die Zugriffsberechtigung kann über User/Passwort-Freigabe oder über einen Eintrag in einen Verzeichnisdienst (Active Directory o.ä.) gelöst werden.

[4] WORM, *write once read many (times)*. Die Eigenschaft, dass einmal geschriebene Daten nicht mehr gelöscht oder überschrieben werden können, wird in diesem Falle softwareseitig realisiert.

[5] CIFS, *Common Internet File System*, wurde 1996 von Microsoft eingeführt und beschreibt eine erweiterte Version von SMB. SMB, *Server Message Block*, ist ein Kommunikationsprotokoll für Datei-, Druck- und andere Serverdienste in Netzwerken.

[6] NFS, *Network File System*, ist ein von Sun Microsystems entwickeltes Protokoll, das den Zugriff auf Dateien über ein Netzwerk ermöglicht.

[7] Ein RAID, *Redundant Array of Independent Disks*, dient zur Organisation mehrerer physischer Festplatten eines Computers zu einem logischen Laufwerk, das eine höhere Datensicherheit bei Ausfall einzelner Festplatten garantiert. Bei RAID 5 ist die Datensicherheit des Arrays beim Ausfall von maximal einer Platte gewährleistet.
RAID 6 funktioniert ähnlich wie RAID 5, verkraftet aber den gleichzeitigen Ausfall von bis zu zwei Festplatten. Bei Ausfall einer Platte kann das Wiederherstellen der Datenredundanz bei 1TB Festplatten bis zu 3 Tage dauern. Bei RAID 5 ist während dieser Zeit kein Schutz vor Datenverlust gegeben.

e) Konfiguration und Administration sollen einfach und menugeführt über eine ***Webschnittstelle*** erfolgen (keine Telnet- oder konsolenbasierte Administration).

f) Vier bis fünf interne ***sATA[8] Platteneinschübe*** für 1000 GB Festplatten sind notwendig. Hot-Swapping /Hot-Plugging[9] bei den Platten ist nicht unbedingt nötig.

g) Eine ***Lese- und Schreibrate*** von minimal 10 MB/s bei RAID 1 sollte erreicht werden.

h) Die Unterstützung von ***NDMP[10]*** ist keine notwendige Voraussetzung.

i) Zur ***Fernüberwachung*** des Systemstatus kann SNMP[11] oder eine einfache eMail-Benachrichtigung eingesetzt werden.

j) Eine ***Redundanz*** im Bereich RAID/Festplatten-Kontroller, Stromversorgung und Netzwerkkarte ist nicht notwendig. Diese Redundanz wird durch die Speicherung auf mehreren Speicherboxen erreicht.

k) Das in der Speicherbox eingesetzte ***Betriebssystem*** (Windows, Linux, FreeNAS, etc.) ist zweitrangig.

l) Eine ***Offenlegung*** der Hardware- und Softwaredetails ist von Vorteil, aber nicht zwingend, die Speicherbox wird als Blackbox[12] eingesetzt.

2.2 Anforderungen Festplatten

a) Aufgrund der Projektvorgaben müssen ***1000 GB sATA Festplatten*** eingesetzt werden. Die meisten Produkte erfüllen die gleichen gängigen Anforderungen (Cache: 32 MB, Kapazität: 1000 GB, Schnittstelle: SATA 3,5", Umdrehungen: 7.200 U/min, Zugriffszeit: 8.5 ms).

b) Hingegen unterscheiden die Hersteller zwischen Desktop- und Server-Speicherplatten. Server-Speicherplatten sollten eine längere Lebensdauer aufweisen und sind für den 7 x 24 Stunden Betrieb ausgelegt, sie kosten aber in der Regel auch ⅓ bis ½ mehr. 1 Mio Stunden ***MTBF[13]*** sollten in unserem Falle mindestens erfüllt werden.

c) Die Speicherplatten müssen zur ***NAS kompatibel*** sein. Eine höhere Sicherheit wird erreicht, wenn nicht beide Speicherboxen mit Platten vom gleichen Hersteller ausgerüstet werden

2.3 Anforderungen USV[14]

a) Eine USV pro Speicherbox soll dafür sorgen, dass die Speicherbox bei einem Stromausfall sicher heruntergefahren wird, dazu wird eine kurze ***Autonomiezeit*** von maximal 5 Minuten benötigt.

b) Die USV soll die angeschlossene Speicherbox auch vor ***Überspannungen***, Spannungsspitzen, Blitzschlag etc. schützen.

c) Die USV muss die Möglichkeit haben, das Herunterfahren der Speicherbox einzuleiten. Wenn ein automatisierter ***Shutdown*** von der Speicherbox nicht unterstützt wird, erübrigt sich eine USV bzw. kann sie durch einen einfachen Überspannungsschutz ersetzt werden.

2.4 Anforderungen Software

a) Die notwendige *Storage Management Software* soll alle Daten von der einen Speicherbox sicher und automatisch auf die zweite Speicherbox replizieren. Die ***Replikation[15]*** soll entweder im Modus Synchronisation (Daten sind auf beiden Speicherboxen identisch) oder WORM (Daten werden nur von A nach B repliziert, in B aber nie gelöscht) möglich sein.

b) Die Software soll periodisch die ***Integrität[16]*** der Daten überprüfen. Diese Überprüfung kann entweder durch Vergleich der Daten auf den beiden Speicherboxen oder durch Berechnen eines Hash-Wertes für jede Datei mit Abgleichen der Werte mit einer Datenbank erfolgen

c) Die Replikation soll fortlaufend erfolgen, der Integritätscheck soll regelmässig stattfinden und automatisch gestartet werden. Dazu muss ein ***Scheduling[17]*** der notwendigen Prozesse möglich sein.

Anmerkung

Die meisten Begriffserklärungen in den Fussnoten stammen von Wikipedia (www.wikipedia.org, deutsch oder englisch).

---

[8] *Serial ATA (auch Serial Advanced Technology Attachment)* ist ein für den Datenaustausch zwischen Prozessor und Festplatte entwickelter Datenbus, Schnittstelle und Stecker an den Festplatten sind normiert.

[9] *Hot Swapping* bedeutet, dass eine Festplatte im laufenden Betrieb gewechselt werden kann.

[10] NDMP, *Network Data Management Protocol*, ist eine standardisierte Schnittstelle, über die es möglich ist, Back-up- und Restore-Operationen von NAS-Servern mit einer Backup-Software zu steuern.

[11] SNMP, *Simple Network Management Protocol*, ist ein Netzwerkprotokoll, um Netzwerkgeräte (z. B. Router, Server, Switches, Drucker, Computer usw.) von einer zentralen Station aus überwachen und steuern zu können.

[12] *Blackbox*, ein im Inneren komplexes System wird nur nach seinen nach aussen tretenden Eigenschaften beurteilt.

[13] MTBF, *Mean Time Between Failures*, ist die Abkürzung für die mittlere Betriebsdauer zwischen Ausfällen.

[14] USV, unterbrechungsfreie Stromversorgung.

[15] Eine bekannte einfache Lösung im Windows Umfeld ist robocopy.exe (*Robust File Copy for Windows*) von Microsoft, beide Replikationsmodi sind hier möglich. Das Tool rsync leistet ähnliches im Linuxumfeld. Es gibt aber auch ausgereiftere kommerzielle Software für die sichere Datenreplizierung über Netzwerke.

[16] Bekannte Lösungen aus dem Linux Umfeld sind für dieses Problem diff, bzw. rdiff, rsync (Synchronisation von Daten über ein Netzwerk) und tripwire (lokale Integritätsprüfung).

[17] Unter *Scheduling*, Zeitablaufsteuerung, versteht man die Erstellung eines Ablaufplanes *(schedule)*, der Prozessen zeitlich begrenzt Ressourcen zuweist.