'Sauver les CD' Speicherbox
Softwarelösung "Replizieren und Validieren"

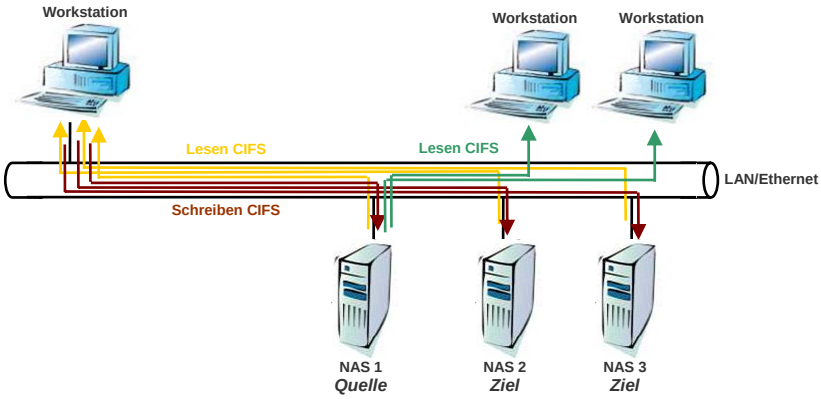
1 Anforderungen

In den Anforderungsspezifikationen zur "Sauver-les-CD" Speicherbox-Lösung haben wir folgende Anforderungen für die Software festgelegt:

a) Die *Storage Management Software* soll alle Daten von der einen Speicherbox sicher und automatisch auf die zweite Speicherbox replizieren. Die ***Replikation***[1] soll entweder im Modus Synchronisation (Daten sind auf beiden Speicherboxen identisch) oder softWORM[2] (Daten werden nur von A nach B repliziert, in B aber nie gelöscht) möglich sein.

b) Die Software soll periodisch die ***Integrität***[3] der Daten überprüfen. Diese Überprüfung kann entweder durch Vergleich der Daten auf den beiden Speicherboxen oder durch Berechnen eines Hash-Wertes für jede Datei und 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***[4] der notwendigen Prozesse möglich sein.



Topologie im Netzwerk: Workstation und drei Speicherboxen

---

[1] *Replikation* oder Replizierung bezeichnet die mehrfache Speicherung von gleichen Daten an unterschiedlichen Speicherorten. Hier ist das einfache Kopieren der Daten von einem Quellspeicherort nach einem Zielspeicherort gemeint.

[2] Mit *SoftWORM* werden im Allgemeinen Systeme bezeichnet, deren Software oder Verwaltungssoftware die *Write-Once*-Eigenschaft erzeugen.

[3] *Integritätsprüfung* bedeutet hier eine regelmässige Kontrolle der Verzeichnisse und Dateien auf unerwartete Veränderungen.

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

2 Replikationssoftware

Zur Replikation kann die bekannte Lösung ***robocopy.exe***[5] *(Robust File Copy for Windows)* von Microsoft eingesetzt werden, beide Replikationsmodi (Synchronisation oder *softWORM*) sind hier möglich. Robocopy kopiert Dateien und Verzeichnisbäume rekursiv. Unterbrochene Kopiervorgänge werden automatisch wieder aufgenommen. Das Tool kopiert nur neue und veränderte Dateien und benutzt zur Erkennung Zeitstempel und Dateigrösse. Geöffnete Dateien können nicht kopiert werden; Robocopy wartet in diesem Falle, bis die Datei wieder geschlossen ist.

Robocopy[6] bietet eine Möglichkeit, den Netzwerkverkehr zu drosseln. Es gibt aber keine Möglichkeit, das Ergebnis des Kopiervorgangs durch erneutes Lesen der kopierten Datei zu validieren (wie z.B. bei copy /verify oder der Option verify ON[7]).

Robocopy im *WORM*[8] Mode bedeutet, dass bereits existierende Dateien und Verzeichnisse im Zielverzeichnis nicht überschrieben werden können:

```
   robocopy  source  destination /E /XC /XN /XO /COPYALL [/IPG:n]

         Usage :: ROBOCOPY  source  destination  [options]
        source :: Source Directory (drive:\path or \\server\share\path)
   destination :: Destination Dir  (drive:\path or \\server\share\path)

:: Copy options ::
             /E :: copy subdirectories, including Empty ones
            /XC :: eXclude Changed files
            /XN :: eXclude Newer files
            /XO :: eXclude Older files
       /COPYALL :: COPY ALL file info (equivalent to /COPY:DATSOU)
         /IPG:n :: Inter-Packet Gap (ms), to free bandwidth on slow lines
```

Robocopy im *MIRROR*[9] Mode synchronisiert beide Dateibäume. Alle allenfalls im Zielverzeichnis bereits bestehenden Verzeichnisse und Dateien, die im Quellverzeichnis nicht mehr existieren, werden gelöscht. Am Ende sind beide Dateibäume identisch, müssen aber auf Dateiebene nicht gleich sein (Dateien mit gleicher Dateigrösse und Zeitstempel werden nicht als unterschiedlich erkannt):

---

[5] Robocopy wird mit dem Microsoft® Windows® Server 2003 Resource Kit ausgeliefert.

[6] Siehe auch: http://en.wikipedia.org/wiki/Robocopy.

[7] Windows Command Notation: Windows Explorer kopiert immer mit der Option verify ON.

[8] WORM ist die Abkürzung für write once read many (times) = "einmal beschreiben, mehrmals lesen". Siehe http://de.wikipedia.org/wiki/WORM.

[9] Mirror (Spiegel) bezeichnet in Computernetzwerken eine exakte Kopie von Daten. Siehe http://de.wikipedia.org/wiki/Mirror.

```
   robocopy  source  destination /MIR /COPYALL[/IPG:n]

          Usage :: ROBOCOPY  source  destination  [options]
         source :: Source Directory (drive:\path or \\server\share\path)
    destination :: Destination Dir  (drive:\path or \\server\share\path)

:: Copy options ::
           /MIR :: MIRror a directory tree (equivalent to /E plus /PURGE)
             /E :: copy subdirectories, including Empty ones
         /PURGE :: delete dest files/dirs that no longer exist in source
       /COPYALL :: COPY ALL file info (equivalent to /COPY:DATSOU)
         /IPG:n :: Inter-Packet Gap (ms), to free bandwidth on slow lines
```

Robocopy kann in einem Durchlauf durch einen Quell-Verzeichnisbaum nicht mehre Zielverzeichnisse aktualisieren. Für jedes Zielverzeichnis muss der Quellbaum erneut abgearbeitet werden

3 Integritätsprüfung

Wenn wir uns für die Integritätssicherung auf das Lesen von Dateien beschränken, sind drei Datei-Vergleichmodi denkbar: Daten auf A und B sind identisch (Verzeichnisstruktur und Dateiinhalt und Zeitstempel); Dateien auf A und B sind gleich (Verzeichnisstruktur und Dateien); und die dritte Möglichkeit, alle Verzeichnisse und Dateien auf A sind identisch oder gleich auf B, es können sich aber auch weitere Verzeichnisse und Dateien auf B befinden. Für die aus archivischer Sicht interessante WORM Lösung der Datenreplikation (Dateien von A nach B kopieren, nicht aber bereits vorhandene Daten auf B gelöscht) ist die dritte Variante der Integritätsprüfung hinreichend und adäquat.

Da Robocopy jeweils nicht alle Verzeichnisse und Dateien liest und vergleicht, sondern sich dabei alleine auf Zeitstempel und Dateigrösse verlässt und auch einen Kopiervorgang nicht zusätzlich durch Dateivergleich verifiziert (copy /verify), ist ein weiteres Programm notwendig, das die Integritätsprüfung in diesem Sinne sicherstellt.

Preisgünstige Hard-/Firmware im NAS-Bereich bietet aber keine regelmässige und automatische Überprüfung der Integrität (Lesbarkeit und Korrektheit) der Blockstruktur auf den Festplatten. Fehler werden erst beim bewussten Lesen oder Schreiben eines Blocks erkannt. Die Geräte stellen zum Lesen der ganzen Festplatte meist einen RAID-Check im Administrationsmodus zur Verfügung. Dabei wird die gesamte Blockstruktur des RAID gelesen; Datenzugriff ist dabei nicht möglich und der Vorgang dauert in der Regel gleich lange wie der Aufbau des entsprechenden RAIDs. Diese Art der Datenüberprüfung ist deshalb recht unpraktisch.

Da für die oben beschriebene Art der Integritätsprüfung (alles auf A identisch auf B) und für das regelmässige Lesen der Daten auf dem RAID kein geeignetes Produkt am Markt gefunden werden konnte, wird eine entsprechende Lösung im Rahmen des Projekts entwickelt.

3.1 Autoverify

Das Programm vergleicht von einem Quellverzeichnis ausgehend rekursiv Verzeichnisstruktur und Dateien mit ein oder mehreren Vergleichsverzeichnissen.

```
autoverify  source  destination1;dest2;dest3
```

Vergleichsverzeichnisse werden mit Strichpunkt verbunden aufgelistet (vergleiche Windows &PATH). Weitere Optionen sind:

– Schreiben einer Logdatei (default *autoverify.log*)
– Meldungen per E-Mail (Mail Server, Port und Adresse)
– Ein Testmail an die angegebene E-Mail Adresse verschicken
– Meldungen am Bildschirm über jede Dateiaktivität (verbose)
– Anzahl Dateiunterschiede die zum Abbruch des Programms führen
– Fortschrittsmeldung per E-Mail nach bestimmter Zeit
– Kopieren fehlender Dateien und Verzeichnisse von Quelle ans Ziel
– Anzeigen von verwaisten Dateien/Verzeichnissen im Ziel
– Verwaiste Dateien/Verzeichnisse im Ziel können virtuell gelöscht werden, d.h. sie werden automatisch umbenannt
– Sleeptime zwischen den Dateizugriffen zur Reduzierung des Netzwerkverkehrs

Damit das Programm bei der zu erwartenden längeren Laufzeit abgebrochen und wieder gestartet werden kann, ist eine Restart Log-Datei notwendig, die beim erneuten Starten des Programms ein Weiterarbeiten vom letzten Haltepunkt aus erlaubt. Haltepunkt ist das zuletzt vollständig gelesene und verglichene Verzeichnis. Ein Restart erfolgt nur bei vorhandener Restart Log-Datei und gleichen Quell- und Vergleichsverzeichnissen.

Bei einem Vergleichsfehler auf Dateiebene wird ein Eintrag in die Logdatei geschrieben (default *autoverify.log*) und bei entsprechender Option ein Mail verschickt.

Bei einem fehlenden Verzeichnis werden die damit fehlenden Unterverzeichnisse und Dateien nicht weiter gesucht und eine Verzeichnisfehlermeldung ausgegeben oder bei der Option COPY mit Hilfe des Programms robocopy.exe die fehlenden Dateien/Verzeichnisse kopiert.

Verwaiste Dateien/Verzeichnisse im Ziel können entweder angezeigt oder mit der Option PURGE umbenannt werden, sodass sie in einem weiteren Programmdurchlauf nicht mehr als verwaist ausgewiesen werden (sie sind dann quasi virtuell gelöscht). Als Marker wird ein *Tilde Number Sign* **~#** verwendet[10].

[10] In Anlehnung an die Bezeichnung von Temporärdateien unter Windows.

Folgende Anwendungsarten und Optionen stehen zur Verfügung:

```
       Usage :: autoverify.exe source destination;dest2;dest3 [options]
      Source :: Source Directory (drive:\path or \\server\share\path)
 Destination :: Directory list to compare and copy
                (drive:\path or drive:\path;drive:\path)

:: Logging Options :
   /LOG:file :: Output to LOG file instead of autoverify.timestamp.log
  /LOG+:file :: Appends to existing LOG file
       /PI:n :: Progress Indicator every n sec: default 10
   /MAIL:receiver's e-mail address:SMTP Server:SMTP account:password:[port]
             :: (Example: /MAIL:m.muster@kost.ch:smtp.kost.ch:muster:12345)
   /TESTMAIL :: Send a test e-mail and do nothing else
      /FMB:n :: Flush Mail Buffer after elapsed time: default 4 hours
    /PMESS:n :: Generate Performance Message after elapsed minutes: default non
        /NMW :: No Mail Warning in case of mismatch incidences
          /V :: Produce Verbose output, show each compared directory
         /VV :: Produce Very Verbose output, show each compared directory & file

:: Syncronize Options :
       /COPY :: Copy missing files and directories to destination with robocopy
      /IPG:n :: Inter-Packet Gap (ms), to free bandwidth on network: default 10
       /PS:n :: Packet Size for data transfer: default 64 kbyte
      /PURGE :: * removes dest files/dirs that no longer exist in source
                by renaming into ~#files/~#dirs
        /NOC :: No Orphan Control on destination file and directory
        /NOD :: No missing Directory processing
        /NOF :: No File verification process - simple directory listing

:: Retry Options :
      /NMI:n :: Number of Mismatch Incidences before shutdown: default 10
    /RSF:file:: Output to Restart File instead of autoverify.rsf
      /RST:n :: Time Restart Information is valid in hrs: default 48
        /R:n :: Number of retries on failed read or copies: default 1 million
        /W:n :: Wait time between retries: default is 30 seconds
       /LOOP :: Loop until terminated with ctrl-c
    /INTERVAL:hh:mm-hh.mm :: Loop only in dedicated time range: from-to

:: Help :
        /VER :: Version number of autoverify
          /? :: Display this help file
```

3.2 Die einzelnen Optionen

Logging Options :

/LOG:filename

Mit dieser Option kann statt *autoverify.timestamp.log* im Arbeitsverzeichnis eine andere Logdatei gewählt werden. /LOG+ verhindert das Überschreiben einer bereits bestehenden Logdatei. /LOG bedeutet keine Logdatei.
Log-Rotation begrenzt im /LOOP oder /INTERVAL Fall die Grösse der Logdatei auf 32 MB. *Log-Rotation* findet jeweils am Ende eine Gesamtdurchlaufes (Loop) statt. Mit der Option /LOG:filename wird die bezeichnete Logdatei jeweils wieder überschrieben. Achtung, die Option /LOG+ schaltet die *Log-Rotation* aus.

/PI

Zur Anzeige des Programmfortschritts wird regelmässig ein Punkt am Bildschirm ausgegeben. Mit /PI oder /PI:0 wird diese Ausgabe abgeschaltet. Der

Punkt wird nicht in die Logdatei geschrieben. Während dem Kopiervorgang mit Robocopy wird kein Fortschrittszeichen geschrieben.

/MAIL

Mit dieser Option wird der Mailversand konfiguriert (analog zum Unixprogramm *sendmail*). Es können mehrere Mailadressen getrennt durch Komma oder Strichpunkt angegeben werden. Notwendig sind weiter ein SMTP Server und ein SMTP-Account mit Passwort. Die Option /TESTMAIL erlaubt den Versand einer Mail zur Überprüfung der Settings, das Programm bricht anschliessend ab.

/FMB

Meldungen per Mail (im Prinzip die gleichen Meldungen wie am Bildschirm und in der Logdatei) werden gepuffert und nur periodisch verschickt. Eine Warnmeldung auf Grund von unterschiedlichen oder fehlenden Dateien oder Verzeichnissen wird sofort mit hoher Priorität verschickt und der Mail Buffer dann auch gleichzeitig geleert. FMB legt die Periodizität für das Verschicken von Statusmails fest. Mit /FMB:0 oder /FMB wird jede Meldung sofort versendet.

/PMESS

Eine Performance-Meldung kann periodisch ausgelöst werden. Die Meldung zeigt den Datendurchsatz seit der letzen Performance-Meldung. Diese Meldung wird mit hoher Priorität verschickt und leert ebenfalls den Mail Buffer. Die Performance-Meldung kann auch und vor allem verwendet werden, um zu kontrollieren ob dass das Programm noch läuft.

/NMW

Eine Warnmeldung auf Grund von unterschiedlichen oder fehlenden Dateien oder Verzeichnissen wird sofort mit hoher Priorität verschickt und der Mail Buffer gleichzeitig geleert. Mit /NMW kann dieses Verhalten abgestellt werden, Warnmeldungen werden dann wie alle andern Log-Einträge im Mailbuffer gespeichert und erst über die Einstellung von /FMB verschickt.

/V

Mit der Option /V wird für jedes verarbeitete Verzeichnis eine Meldung generiert. Mit /VV wird für jede verarbeitete Datei eine Meldung erzeugt. Meldungen bestehen aus einem Datums-/Zeitstempel und einem Meldungstext und werden am Bildschirm, in die Logdatei und gegebenenfalls auch per Mail ausgegeben.

Syncronize Options :

/COPY

Mit dieser Option werden auf der Ziel-Speicherbox fehlende Dateien und Verzeichnisse mit *robocopy.exe* kopiert. Anschliessend werden die kopierten Dateien und Verzeichnisse durch Lesen und Vergleichen überprüft. Diese Überprüfung lässt sich mit /NOF abschalten. Während des Kopiervorgangs werden keine Fortschrittszeichen ausgegeben, Robocopy-Programmausgaben erscheinen mit den Optionen /V und /VV nur am Bildschirm und nicht in der Logdatei. Abgebrochene Kopiervorgänge werden mit der Option /COPY automatisch wieder aufgenommen.

/IPG:n

Diese Option schaltet zwischen das Lesen und Schreiben von 64 KByte Blöcken eine *Sleep* Pause. Damit werden Netzwerkbandbreite und Rechenzeit frei-

gegeben. Die Defaulteinstellung 10 ms verlangsamt den Durchsatz merklich. *Sleep* kann mit /IPG oder /IPG:0 ganz ausgeschaltet werden.

/PS:n

Mit /PS kann die Gösse der Les- und Schreibblöcke in KByte verändert werden. Defaulteinstellung ist 64 KByte.

/PURGE

(noch nicht implementiert) Dateien und Verzeichnisse, welche auf der Quell-Speicherbox nicht mehr existieren, werden in den Zielboxen umbenannt durch ein *tilde-number-sign* (**~#**) vor dem ursprünglichen Dateinamen. Mit der Option /PURGE werden so gekennzeichnete Dateien und Verzeichnisse nicht weiter als Waisen gemeldet.

/NOC

Mit /NOC wird die Anzeige von Waisen auf den Ziel-Speicherboxen ausgeschaltet.

/NOD

Mit /NOD wird die Anzeige von fehlenden Verzeichnissen auf den Ziel-Speicherboxen ausgeschaltet.

/NOF

Mit /NOF wird das Vergleichen von Dateien zwischen Quelle und Ziel-Speicherboxen ausgeschaltet.

Retry Options :

/NMI:n

/NMI legt fest, nach wie vielen Warnungen zu Datei-Mismatch, fehlenden Verzeichnissen oder Waisen das Programm beendet werden soll. /NMI ohne Zähler bedeutet: kein Programmabbruch

/RSF:file

Die Restartdatei *autoverify.rsf* kann durch eine Datei mit anderem Namen ersetzt werden.

/RST:n

Ein Restart beginnt mit dem zuletzt vollständig verarbeiteten Verzeichnis. Voraussetzung sind beim Programmaufruf gleiche Quell- und Zielparameter, gleiches Arbeitsverzeichnis, gleicher Arbeitsrechner und Programmabbruch nicht länger zurück als 48 Stunden. /RST schaltet den Restart aus.

/R:n

/R legt fest, wie viele Male versucht werden soll, eine Datei zu lesen. Der Defaultwert ist 1 Million.

/W:n

Wenn eine Datei nicht gelesen werden kann, wird vor einem erneuten Leseversuch eine Wartezeit eingeschaltet, welche durch /W spezifiziert werden kann. Der Defaultwert ist 30 Sekunden.

/LOOP

Das Programm wird nach dem rekursiven Durchgang durch den Quell-Dateibaum automatisch wieder gestartet. Wird keine Logdatei angegeben, wird bei jedem Durchgang eine neue Logdatei angelegt.

/INTERVAL:hh:mm-hh.mm

Gleiches Programmverhalten wie bei LOOP. Die Programmausführung ist pro Tag auf die Zeit von bis in Stunden:Minuten beschränkt (Genauigkeit 1 Minute). Als einzige Programmaktivität wird ausserhalb der Ausführungszeit die Perfomancemeldung wie mit PMESS spezifiziert ausgegeben. PMESS kann damit zur Überwachung des Betriebszustandes eingesetzt werden.

Help :

/VER

Die Programmversion wird zusammen mit der Help-Information angezeigt.

/?

Die Hilfedatei wird am Bildschirm ausgegeben.

3.3 Autoverify Konfigurationen

Gewisse Standardkonfigurationen können einfache Bedürfnisse erfüllen. Im Beispiel ist //quelle/data die Speicherbox, auf welche der Archivadministrator die zu speichernden Daten legt, //ziel/data die Speicherbox für die Replikation (//ziel_1/data;//ziel_2/data;//ziel_3/data ist ebenfalls möglich).

Z.B. kopiert folgende Anweisung alle Daten von der Quelle auf das Ziel ohne weitere Kontrolle und ohne Log Datei (was in etwa dem einfachen Robocopy-Befehl entspricht). IPG:0 bzw. IPG bedeutet kopieren ohne Verzögerung:

```
autoverify.exe //quelle/data //ziel/data /copy /noc /nof /log /ipg
```

Beispiel einer realistischeren Installation im Verzeichnis Startup:

```
autoverify.exe //quelle/data //ziel/data
     /mail:m.muster@kost.ch:smtp.kost.ch:account:passwd
     /pi /v /pmess:120 /nmi /copy /loop
```

Hier werden alle Verzeichnisse und Dateien fortlaufend von //quelle/data nach //ziel/data synchronisiert und regelmässig wieder gelesen. Es wird jedes verarbeitete Verzeichnis ins Logfile geschrieben und alle 2 Stunden eine Performancemeldung generiert. (Es können auch mehrere Mailempfänger angegeben werden.) NMI:0 bzw. NMI verhindert den Abbruch nach einer bestimmten Anzahl von generierten *file-mismatch* Meldungen.

4 Zeitsteuerung (Scheduling)

Prozesse auf Windowsrechnern zeitabhängig zu starten oder stoppen, ist von der korrekten Installation des Windows Schedule Service (Task Scheduler[11]) abhängig, was nur mit Administrationsrechten erfolgen kann. Um keine direkte Abhängigkeit mit der Windowsinstallation und Rechtevergabe auf dem Arbeitsrechner des Archivinformatikers herzustellen, muss ein eigenes einfaches Scheduling vorgesehen werden.

Mit der Option LOOP kann in *autoverify* ein einfaches Scheduling konfiguriert werden. Der Programmstart erfolgt über den Ordner *Startup* oder *Autostart* in *Programme* auf dem Rechner des Archivinformatikers. Mit der Option LOOP

[11] *at.exe* auf Windows NT Systemen, *schtasks.exe* ab Windows XP, http://en.wikipedia.org/wiki/At_(Windows)

wird *autoverify* fortwährend ausgeführt, durchwandert rekursiv den Quell-Dateibaum und vergleicht die Dateien von Quelle und Ziel. Mit der Option COPY werden fehlende Dateien auch gleich kopiert.

Zu diesem Zweck müssen Quell- und Zielspeicherbox an diesem Rechner mit einem Laufwerkbuchstaben verbunden sein. Die Freigabe der zweiten Box soll auf jeden Fall nur auf diesem Rechner erfolgen.

Durch die Restartfähigkeit der beiden Programme kann dieser Rechner jederzeit (abends und am Wochenende) abgeschaltet werden. Der Archivinformatiker erhält per E-Mail vom Fortschritt der Programme Kenntnis.