

Individuelle Praxisarbeit (IPA)

Client Backup Services Zentral und lokales Backup in der Trivadis AG



1 Inhaltsverzeichnis

Teil 1

| | | |
|-----|------------------------------------|----|
| 1 | Aufgabenstellung..... | 5 |
| 1.1 | Ausgangslage..... | 5 |
| 1.2 | Detaillierte Aufgabenstellung..... | 5 |
| 2 | Vorkenntnisse..... | 5 |
| 3 | Vorarbeiten..... | 6 |
| 4 | Firmenstandards..... | 6 |
| 5 | Arbeitsprotokoll..... | 6 |
| 5.1 | .1. Tag (13.3.06)..... | 6 |
| 5.2 | 2. Tag (14.3.06/16.3.06)..... | 6 |
| 5.3 | 3. Tag (16.3.06/17.3.06)..... | 7 |
| 5.4 | 4. Tag (17.3.06/20.3.06)..... | 7 |
| 5.5 | 5.Tag (20.3.06/21.3.06)..... | 8 |
| 5.6 | 6.Tag (23.3.06)..... | 8 |
| 5.7 | 7. Tag (24.3.06)..... | 9 |
| 5.8 | 8. Tag (27.3)..... | 9 |
| 6 | Zeitplan..... | 11 |
| 6.1 | SOLL..... | 11 |
| 6.2 | IST..... | 12 |
| 6.3 | Legende..... | 13 |

Teil2

| | | |
|-------|---|----|
| 7 | Evaluation..... | 15 |
| 7.1 | Mitarbeiterumfrage..... | 15 |
| 7.1.1 | Zentral oder lokal..... | 15 |
| 7.1.2 | Gesamtsystem oder nur Datenbackup..... | 15 |
| 7.1.3 | Zeit für Backup / Zeit für Restore..... | 16 |
| 7.1.4 | Backuphäufigkeit..... | 16 |
| 7.1.5 | Abgedeckte Zeit des Backups..... | 16 |
| 7.1.6 | Backup im laufenden Betrieb..... | 17 |
| 7.1.7 | Momentane Backuplösung..... | 17 |
| 7.2 | Bedingungen..... | 17 |
| 7.3 | Zentrales Backup..... | 18 |
| 7.3.1 | Anforderungen..... | 18 |
| 7.3.2 | Bewertungskriterien..... | 18 |
| 7.3.3 | Bewertung..... | 19 |
| 7.3.4 | Resultat..... | 21 |
| 7.4 | Lokales Backup..... | 21 |
| 7.4.1 | Anforderungen..... | 21 |
| 7.4.2 | Bewertung..... | 23 |
| 7.4.3 | Resultat..... | 26 |

- 8 Realisierung.....
- 8.1 Aufsetzen der Testumgebung.....
 - 8.1.1 Windows-Client.....
 - 8.1.2 Linux Client.....
 - 8.1.3 Server.....
 - 8.1.4 Netzwerkschema.....
- 8.2 Konfiguration der Testumgebung.....
 - 8.2.1 Dienste.....
 - 8.2.2 SSH und Key-Exchange.....
 - 8.2.3 Integration ins Trivadis Backupkonzept.....
- 8.3 BackupPC.....
 - 8.3.1 Installation.....
 - 8.3.2 Konfigurationsfiles.....
 - 8.3.3 Host finden.....
 - 8.3.4 Limitationen.....
 - 8.3.5 Datenübertragung.....
 - 8.3.6 Versionisierung.....
 - 8.3.7 Zeitmanagement.....
 - 8.3.8 Pooling.....
 - 8.3.9 Kompression.....
 - 8.3.10 Quota (Speicherplatzbeschränkung).....
 - 8.3.11 Konzepte.....
- 8.4 Lokale Backup Lösung.....
 - 8.4.1 Imaging.....
 - 8.4.2 Datenbackup.....
- 8.5 Security.....
 - 8.5.1 Berechtigungen.....
 - 8.5.2 Login.....
 - 8.5.3 Dienste.....
- 9 Testen.....
- 9.1 Testfälle.....
 - 9.1.1 Zentrales Backup.....
 - 9.1.2 Lokales Backup.....
- 9.2 Ergebnisse.....
- 10 Literaturverzeichnis.....
- 11 Glossar.....
- 12 Anhang.....

Teil 1:

Umfeld und Ablauf

2 Aufgabenstellung

2.1 Ausgangslage

Trivadis hat 400 Notebooks im Einsatz. Backup von Daten und gesamter Konfiguration liegt in der Eigenverantwortung der Mitarbeiter. Dies wird aber leider nur selten wirklich konsequent umgesetzt, weil teilweise die technischen Mittel nicht genutzt werden, resp. das Wissen um die Dringlichkeit für Backup nicht mit genügender Beachtung gelebt wird. Jeder Mitarbeiter könnte eine USB/FW Disk anfordern und/oder Daten auf die zentralen Ablagen tvd_all / Userhome stellen.

2.2 Detaillierte Aufgabenstellung

Es sollen den Mitarbeitern einfache Services angeboten werden, die sie dazu motiviert regelmässig Backup von Konfiguration und/oder mindestens der Daten zu machen.

Abgrenzung: Client-Backup liegt weiterhin in der Eigenverantwortung des MA.

Aufgaben IPA :

- Anforderungen einholen, gewichten und Evaluationskriterien erstellen
- Aufbau der Lösung(en) und Test mind. der aufgeführten Kriterien
- Standardisierung der Lösung für persönliche Backup auf USB/FW Disk. Kriterien dazu sind mind.:
 - Automatisiertes Backup nach Zeitperiode
 - Möglichkeit für One Touch Image Backup
 - Erstellen von Versionen
 - Einzelne Files Backup / Restore Möglichkeit
 - Client und OS unabhängig oder 2 Lösungen
- Standardisierung der Lösung für Online/Netshare Backup. Kriterien dazu sind mind.:
 - Automatisiertes Backup definierter Files/Daten nach Zeitperiode
 - Userquota / Filesize Limit
 - Erstellen von Versionen
 - Client und OS unabhängig oder 2 Lösungen
 - Einzelne Files Backup / Restore Möglichkeit
 - Integration ins Trivadis – Backupkonzept
 - Online / WebInterface
- Installationsanleitungen erstellen und Helpdesk schulen
- Kommunikation / Marketing an tvd_all

3 Vorkenntnisse

- Systemtechnik Basics seit Anfang der Lehre
- Imaging mit Ghost (o.ä.) seit Anfang Lehre genutzt
- Evaluation und Test von Lösungen und Standard-Produkten

4 Vorarbeiten

- Einarbeiten in aktuelle Lösungen
- Evaluation der zentralen Backuplösung
- Beschaffen der Server/Client-Infrastruktur

5 Firmenstandards

Für dieses Dokument wurde eine Firmenvorlage für Dokumentationen verwendet, die als Schriftart „CG Omega“ benutzt.

Für die Installationen wurden Firmenstandard-Installation verwendet (Linux gemäss Firmen-Anleitung; Windows gemäss Standard-Image).

6 Arbeitsprotokoll

6.1 .1. Tag (13.3.06)

Als ich meine IPA begann hatte ich noch keine konkreten Vorstellungen vom Aufbau. Durch meine Vorarbeiten wusste ich schon welche Lösungen ich entwickeln würde. Ich beschloss erst einmal einen Zeitplan zu erstellen und meine Arbeitsschritte festzuhalten. Meine Aufgabenstellung und der Kriterienkatalog unterstützten mich dabei.

Ich begann dann die beiden Clients aufzusetzen, was kein Problem darstellte und mehr oder wenig nur eine Zeitfrage war (für den Windows-Client hatte ich ein Image, welches ich nur minimal konfigurieren musste und Open SuSE 10.0 habe ich die Installation-DVD benutzt).

Der Server war da schon etwas aufwändiger. Mit Hilfe von Knoppix installierte ich Gentoo. Ausser einem kleinen Problem mit dem Bootloader (siehe Dokumentation) ging alles glatt.

Die Konfiguration und die Software-Installationen werde ich morgen noch fertig stellen.

6.2 2. Tag (14.3.06/16.3.06)

Der zweite Tag stand ganz im Zeichen des Konfigurierens. Um den Server sauber zu betreiben sind einige Dienste unabdingbar:

- Syslog (sysklogd)
- Cron (fcron)
- Mail (sendmail)
- Webserver (Apache mit CGI/mod_perl/LDAP)

- Samba (Client/Server)
- Remotezugriff (sshd von OpenSSH)

Die verschiedenen Dienste mussten konfiguriert und vorbereitet werden um nachher dem Server dienen.

Um ein komfortables Suchen zu ermöglichen, habe ich slocate installiert, welches eine Filesuche auf Indexbasis zulässt. Der Index wird täglich erstellt via Cronjob.

Der Mailserver dient nur zum lokalen Mailversand eines Programms an beispielsweise „root“. Samba habe ich installiert gemäss Empfehlung der BackupPC-Dokumentation, so dass ich die Möglichkeit habe auf einen SMB-Share zuzugreifen.

Den Apache-Webserver habe ich noch nicht abschliessend konfiguriert sondern erstmal eingerichtet und die grundsätzlichen Einstellungen vorgenommen (User, Port, Pfade, MPM usw.).

SSH ist für die Administration unabdingbar auch lassen sich mittels SCP (SecureCopy) auf sicherem und eifachem Weg Daten vom/zum Server kopieren.

6.3 3. Tag (16.3.06/17.3.06)

Am 3. Tag habe ich begonnen mit der Konfiguration von BackupPC. Ich war etwas früher dran als ursprünglich gedacht. Die Grundinstallation klappte, ich musste aber einige Punkte aus der BackupPC-Dokumentation bei mir anders machen. Es werden zahlreiche Einträge im mod_perl.conf File aufgelistet, mit denen aber Apache nicht mehr klar kommt. Nach langem Suchen (mit Hilfe von Dani Steiner) hab ich dort schliesslich den Fehler festmachen können.

Ich konnte bereits ein erstes erfolgreiches Backup erstellen nach 2 Konzepten (Vergleiche 8.3.12 Konzepte). Die Kompression tat ihren Teil und die 12GB Daten wurden auf 7GB geschrumpft. Dank dem Pooling (Vergleiche 8.3.6 Versionisierung) sollten andere Windows XP-Backups nun nicht mehr so viel Platz brauchen. Bei der Dokumentation hatte ich einige Probleme da mir keine Struktur so richtig gefiel. Allgemein glaube ich bald einen Schreib-Block einlegen zu müssen, da sonst die Balance zwischen Theorie und Praxis nicht mehr stimmt.

6.4 4. Tag (17.3.06/20.3.06)

Der 4. Tag stand im Zeichen von LDAP. Ich habe mir gedacht, dass sich alle User einloggen können und ihr jeweiliges Backup zu sehen und zu starten arbeite ich mit unserem LDAP-Server.

Von Thomas Weber (LDAP-Verantwortlicher) habe ich die benötigten Angaben bekommen (in der httpd.conf von Apache):

```
-----  
AuthType Basic  
AuthName "Trivadis"  
AuthLDAPAuthoritative on  
AuthLDAPRemoteUserIsDN off  
AuthLDAPDereferenceAliases never  
-----
```

```
| AuthLDAPUrl ldaps://donar.trivadis.com:636/dc=trivadis,dc=com?uid? |  
| sub? |  
|----- require valid-user -----|
```

Der Apache hatte zu diesem Zeitpunkt jedoch noch keine LDAP-Untersützung, also musste ich den erstmal neu kompilieren. Neu brauchte ich auch noch das Apache-Modul `mod_auth_ldap` welches ich via Gentoo-Package-System (Portage) installiert habe.

Eine Verbindung zum Server war aber einfach nicht möglich. Im Log stand Folgendes:

```
|-----|  
| [Fri Mar 17 11:31:27 2006] [notice] LDAP: Built with OpenLDAP LDAP SDK |  
| [Fri Mar 17 11:31:27 2006] [notice] LDAP: SSL support unavailable |  
| [Fri Mar 17 11:31:27 2006] [warn] [client 172.16.52.42] [7436] auth_ldap |  
| authenticate: user sto authentication failed; URI /cgi-bin/BackupPC_Admin |  
| [LDAP: ssl connections not supported][Can't contact LDAP server] |  
|-----|
```

Beim Start von Apache reklamierte dieser immer, er kenne einige LDAP-Direktiven nicht. Via <http://localhost/server-info> (direkt auf dem Server ausgeführt) konnte ich sehen, dass das geladene `mod_auth_ldap` diese Direktiven auch tatsächlich nicht hatte.

Der LDAP-Verantwortliche kannte diesen Fehler auch nicht, da es bei ihm mit dem Apache-Modul und SSL auf Anhieb geklappt hatte.

Nach langem Suchen schliesslich fand ich heraus, dass das Modul welches ich hinzugefügt hatte, das Apache-Standardmodul überschrieben hatte, welches den Support für SSL und die gewünschten Direktiven.

Der SSL-Support ist noch immer nicht möglich, aber über das normale LDAP kann sich der User nun bei BackupPC anmelden.

6.5 5.Tag (20.3.06/21.3.06)

Der erste Teil des 5. Tages verlief ähnlich wie der vierte Tag. Ich versuche LDAP over SSL zum Laufen zu kriegen, musste aber schliesslich aufgeben.

Ich habe für die verschiedenen Backup-Varianten Config-Files erstellt, die je nach Wunsch des Users per Symlink verknüpft werden.

Als Standard ist ein Windows-Backup über Samba eingerichtet, dass die ganze Partition C backupt. Diese Konfiguration wird voraussichtlich auch die häufigste sein. Daneben habe ich die Konfiguration für Linux (über `rsync`) eingerichtet und erfolgreich getestet.

Das ganze IPA-Dokument hat nun eine neue Struktur, die ich gemäss dem FA-Dokument gewählt habe.

6.6 6.Tag (23.3.06)

Leider war ich beim testen der Linux-Variante am 5. Tag etwas vorschnell: Ich mich zwar einloggen und ein Backup starten. Dies brach jedoch nach ca. 5min ab mit

einem „Connection timeout“. Ich vermute, dass gar kein Backup gestartet wird, sondern nur der Prozess angestossen wird, der dann ins Leere läuft.

Ich habe parallel begonnen mit der Evaluation der lokalen Backup-Lösung und habe die wichtigsten Punkte notiert und bewertet. Ebenfalls erstellt habe ich die ersten Testfälle. Ich behandle dabei die lokale und die zentrale Lösung separat. Ich habe versucht möglichst logisch vorzugehen, von den ersten Schritten über das Backup zum Restore. Ich habe auch eine Tabelle erstellt, die dann die Ergebnisse der Testfälle festhalten soll.

Da Modelle helfen komplexe Systeme und Zusammenhänge zu verstehen und zu veranschaulichen habe ich begonnen (auf Rat meines Fachvorgesetzten) einige Grafiken zu erstellen mit Visio.

Auf der CGI-Seite funktioniert nun die Rechte Vergabe wie sie sollte. Ist ein User als User eines Clients eingetragen, sieht er diesen in der Liste und hat die Berechtigung Backups und Restores zu starten. Der definierte CGI-Admin kann sich einloggen und hat keinerlei Zugriff auf die Daten. Er sieht die Logfiles und die Serverkonfiguration. Ebenfalls hat er die Möglichkeit ein aktualisiertes Config-File nachzuladen.

Ich habe den Zeitplan nochmals etwas angepasst und kann jetzt schon sagen, dass ich die Pufferzeiten gut gebrauchen kann.

6.7 7. Tag (24.3.06)

Der siebte Tag war sehr Durchmischt mit den Aufgaben. Ich habe sowohl nach weiteren Lösungen gesucht um BackupPC unter Linux zum laufen zu bringen und bin dabei schon ein Stück weiter gekommen. Mit dem Tool ssh-keygen habe ich auf dem BackupPC-Server einen Key generiert und diesen auf den Client verteilt (in die Datei ~/.ssh/authorized_keys2). Somit gelingt der Login ohne Passwort und die erste Hürde scheint geschafft. Das Problem ist nun, dass ich auf der Kommandozeile zwar das Backup ausführen kann, BackupPC kann es allerdings noch nicht aus eigener Kraft.

Der weiteren habe ich noch an der Verbesserung der Evaluation gearbeitet, die nun ein eindeutiges Resultat zeigt.

Am Nachmittag war der zweite Expertenbesuch, der mich sehr nervös machte, da ich Angst hatte, bisher zu wenig in die Dokumentation investiert zu haben (wegen den diversen Problemen die ich bishher hatte). Herr Ziegler hat mir allerdings diese Angst genommen und mir gute Tipps zur Verbesserung der Arbeit gegeben. Trotz allem muss ich nun intensiv an meiner Doku feilen und sie schnellstmöglich in eine fertige Form bringen.

6.8 8. Tag (27.3)

Leider viel später als ich gehofft hatte, habe ich die gesamte zentrale Backup-Lösung zum laufen gebracht. Sowohl Windows als auch Linux lassen sich über Samba bzw. über rsync sichern. Der Job lässt sich manuell starten oder wird gemäss dem definierten Zeitrahmen automatisch gestartet.

Leider läuft das Mailsystem nicht, dies hat allerdings nichts mit dem Server zu tun sondern mit der Implementierung der Mails in BackupPC. Dort ist es nämlich nur möglich Mails an eine Adresse in der Form von <loginname>@<domain> zu schicken. In der Trivadis entspricht aber der Loginname nicht dem ersten Teil der Mailadresse, dadurch läuft dieser Job ins Leere.

Weiter habe ich die meisten Testfälle geschrieben und muss diese nun noch testen. Auch habe ich noch weitere Grafiken erstellt die die erklärten Vorgänge und Mechanismen vereinfacht darstellen.

6.9 9. Tag (30.3)

Am 9. Tag hat der Endspurt begonnen. Ich habe zuerst nur einen riesen Berg Arbeit vor mir gesehen, nachdem ich aber alles ein wenig aufgeteilt hatte, war es gar nicht mehr so schlimm. Ich habe die Diagramme zu den Mitarbeiterumfragen erstellt, die nun auch visuell sehr deutlich zeigen, wie breitgefächert meine Lösung sein muss.

Das Dokument steht nun vollständig, es fehlen noch einige Testfälle und die Anleitungen müssen nochmals etwas überarbeitet werden.

Das ganze Dokument hat nun keine Lücken mehr, die ich vor mich her geschoben hatte und das ganze Konzept ist niedergeschrieben.

Ich habe ein neues Kapitel Security erstellt in dem in speziell auf einige Punkte bezüglich der Sicherheitsaspekte meiner Lösung eingehe. Für den Zeitplan habe ich neben dem längst erstellten SOLL nun auch noch den IST-Plan erstellt, der doch einiges Abweicht, schlussendlich aber doch rechtzeitig den Abschluss schafft. Einige Punkte brauchten einfach nicht so lange wie ich geplant hatte, andere benötigten viel länger meine Aufmerksamkeit als ich dachte.

Die Installation und Konfiguration der verschiedenen Komponenten habe ich nun auch fertig dokumentiert, so dass sie jederzeit wiederholbar sind.

Für das zentrale Backup habe ich nun auch noch eine Übersichtstabelle erstellt so dass die wichtigsten Informationen die zum Entscheid geführt haben ersichtlich sind und die beiden Evaluationen einheitlich daher kommen.

Nun habe ich doch eine stolze Anzahl Seiten, so dass ich die Anleitung in den Anhang verschieben kann.

7 Zeitplan

7.1 SOLL

| Aufgaben / Tag | 1 (13.3) | 2 (14.3/16.3) | 3 (16.3/17.3) | 4 (17.3/20.3) | 5 (20.3/21.3) | 6 (23.3) | 7 (24.3) | 8 (27.3) | 9 (30.3) | 10 (31.3) |
|------------------------------------|-------------|------------------|------------------|------------------|------------------|-------------|-------------|-------------|-------------|--------------|
| Planung | | | | | | | | | | |
| Zeitplan erstellen | ■ | ■ | | | | | | | | |
| Zeitplan prüfen (ggf. anpassen) | | ■ | ■ | ■ | ■ | ■ | | | | |
| Arbeitsplatz einrichten | ■ | | | | | | | | | |
| IPA Dokumente lesen | ■ | ■ | | | | | | | | |
| Einarbeiten in BackupPC | | ■ | ■ | ■ | ■ | ■ | | | | |
| Realisierung | | | | | | | | | | |
| Aufsetzen der Testumgebung | ■ | ■ | ■ | | | | | | | |
| Konfiguration der Testumgebung | | ■ | ■ | ■ | ■ | | | | | |
| Konfiguration für zentrales Backup | | | | ■ | ■ | ■ | ■ | | | |
| Lokale Backup-Lösungen vergleichen | | | | | | ■ | ■ | ■ | ■ | |
| Dokumentation | | | | | | | | | | |
| Dokumentvorlage erstellen | ■ | ■ | | | | | | | | |
| Arbeitsjournal | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ |
| Dokumentation schreiben | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ |
| Step-By-Step Anleitung erstellen | | | | | | | ■ | ■ | ■ | |

| | | | | | | | | | | | | | | | | | | | | |
|----------------------------|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|
| Testen | | | | | | | | | | | | | | | | | | | | |
| Testfälle erstellen | | | | | | | | | | | | | | | | | | | | |
| Testen der Testfälle | | | | | | | | | | | | | | | | | | | | |
| Sonstiges | | | | | | | | | | | | | | | | | | | | |
| Besuche des Experten | | | | | | | | | | | | | | | | | | | | |
| Unvorhergesehenes (Puffer) | | | | | | | | | | | | | | | | | | | | |

7.2 IST

| Aufgaben / Tag | 1 (13.3) | 2 (14.3/16.3) | 3 (16.3/17.3) | 4 (17.3/20.3) | 5 (20.3/21.3) | 6 (23.3) | 7 (24.3) | 8 (27.3) | 9 (30.3) | 10 (31.3) |
|------------------------------------|-------------|------------------|------------------|------------------|------------------|-------------|-------------|-------------|-------------|--------------|
| Planung | | | | | | | | | | |
| Zeitplan erstellen | | | | | | | | | | |
| Zeitplan prüfen (ggf. anpassen) | | | | | | | | | | |
| Arbeitsplatz einrichten | | | | | | | | | | |
| IPA Dokumente lesen | | | | | | | | | | |
| Einarbeiten in BackupPC | | | | | | | | | | |
| Realisierung | | | | | | | | | | |
| Aufsetzen der Testumgebung | | | | | | | | | | |
| Konfiguration der Testumgebung | | | | | | | | | | |
| Konfiguration für zentrales Backup | | | | | | | | | | |
| Lokale Backup-Lösungen vergleichen | | | | | | | | | | |
| Dokumentation | | | | | | | | | | |

| | | | | | | | | | | | | | | | | | | | | |
|----------------------------------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Dokumentvorlage erstellen | ■ | ■ | | | | | | | | | | | | | | | | | | |
| Arbeitsjournal | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ |
| Dokumentation schreiben | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ |
| Step-By-Step Anleitung erstellen | | | | | | | | | | | | | | | | | | | | |
| Testen | | | | | | | | | | | | | | | | | | | | |
| Testfälle erstellen | | | | | | | | | | | | | | | | | | | | |
| Testen der Testfälle | | | | | | | | | | | | | | | | | | | | |
| Sonstiges | | | | | | | | | | | | | | | | | | | | |
| Besuche des Experten | | | | | | | | | | | | | | | | | | | | |
| Unvorhergesehenes (Puffer) | | | | | | | | | | | | | | | | | | | | |

7.3 Legende

- Planungsarbeiten
- Realisation, Umsetzen der Planung
- Schreivarbeiten (Dokumentation, Arbeitsjournal und Step-by-Step Anleitung)
- Testen
- Sonstiges
- Entsprechender Punkt ist weggefallen
- Entsprechender Punkt ist neu dazugekommen

Teil 2: Projekt

8 Evaluation

8.1 Mitarbeiterumfrage

Im Vorfeld meiner Facharbeit wollte ich wissen, was für eine Lösung überhaupt gefragt ist, d.h. ich wollte die Bedürfnisse abklären.

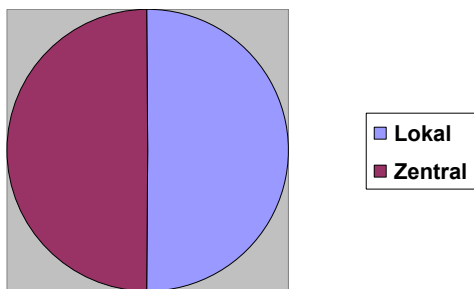
Ebenfalls wollte ich erfassen welche Kriterien als kritisch und welche eher optional zu Betrachten sind.

Mein Fragenkatalog sah so aus:

1. Soll das Backup zentral erfolgen (z.B. auf einen Server) oder lieber auf eine lokale Disk o.ä?
2. Reicht es die Daten zu sichern oder ist eine Sicherung des gesamten Systems erforderlich?
3. Wie lange darf ein Backup/Restore dauern? Wie häufig sollte Backup gemacht werden?
4. Wie lange muss ein Backup zurückreichen?
5. Muss Backup im laufenden Betrieb möglich sein?
6. Welche Backuplösung setzt du momentan ein?

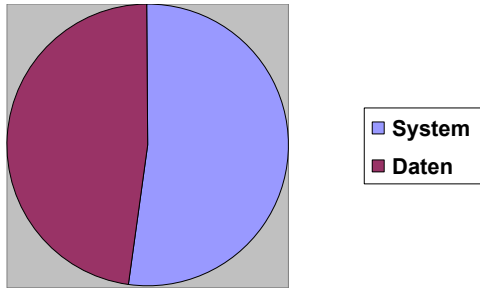
Leider ergab sich aus den Antworten kein klares Bild, so dass meine Lösung relativ breit gefächert sein muss:

8.1.1 Zentral oder lokal



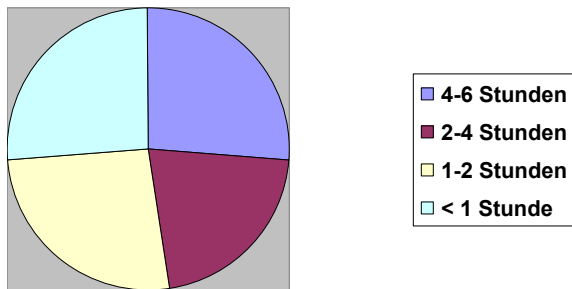
Die eine Hälfte will ein lokales Backup und die andere ein Zentrales.

8.1.2 Gesamtsystem oder nur Datenbackup



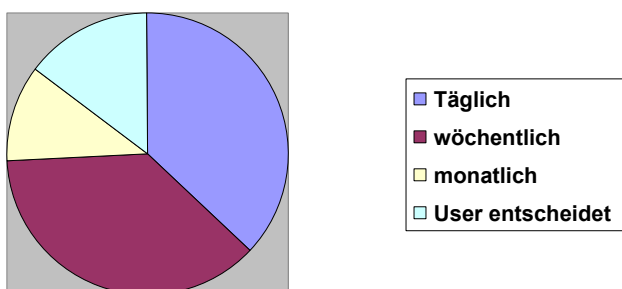
Auch hier ist man sich nicht einig: Wieder wollen jeweils fast die Hälfte das ganze System sichern bzw. nur Datenbackup erstellen.

8.1.3 Zeit für Backup / Zeit für Restore



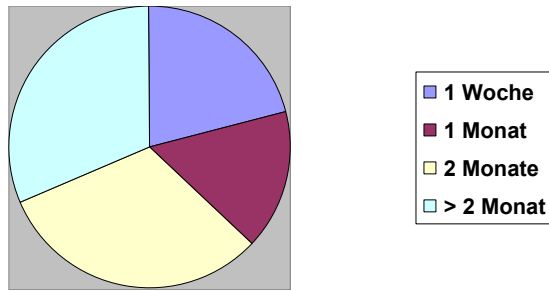
Hier wurde das regelmässige Backup gezählt. Einige Mitarbeiter hatten geschrieben, dass es erstmalig gerne lange dauern darf, dann aber mit den Incrementals sollte es schneller gehen.

8.1.4 Backuphäufigkeit



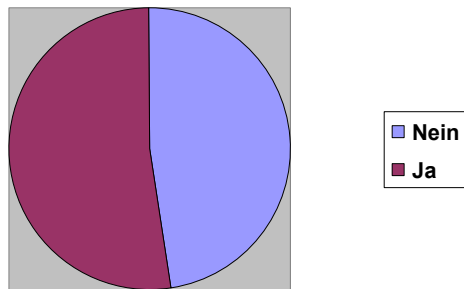
Es scheinen sich die meisten bewusst zu sein, dass täglich das Optimum ist, wöchentlich jedoch realistischer ist, gerade wenn jeweils ein Image erstellt wird.

8.1.5 Abgedeckte Zeit des Backups



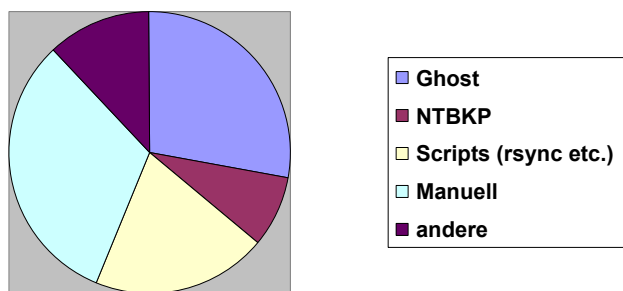
Viele möchten nur 1-3 Versionen speichern, andere wollen dann gerade 10 Jahre zurückreichende Backups (Extremfall).

8.1.6 Backup im laufenden Betrieb



Arbeiten und backupen gleichzeitig? Die Hälfte ist dafür, die andere dagegen.

8.1.7 Momentane Backuplösung



Der grösste Teil benutzt momentan keine Lösung, sondern sichert die Daten sporadisch selbst auf einen Netshare. Dies birgt die grosser Gefahr es zu vergessen. CD's sind als Backup-Medium anscheinend sehr beliebt, evtl. lässt sich so etwas realisieren.

8.2 Bedingungen

Als Grundlage für die Evaluation dienen die Standard-Rechner mit einigen Standardapplikationen wie ein Office-Paket, Browser, Firewall und Anti-Virus Software (nur Windows).

Für das Backup wurde eine 200GB Maxtor Storage Disk genommen die via USB 2.0 mit dem jeweiligen Client verbunden ist.

Die Gewichtung erfolgt nach einem einfachen Prinzip:

- 1 = nice to have
- 2 = kann eine Rolle spielen
- 3 = sehr wichtiger, zentraler Punkt

Anhand diverser Kriterien wurden die Programme geprüft.

Einige Punkte sind nicht so stark bewertet, da evtl. die Möglichkeit besteht, für verschiedene Betriebssysteme andere Lösungen zu verwenden („Betriebssystem“, „Dateisystem“). Dennoch wäre es wünschenswert wenn ein Produkt alle Betriebssysteme abdecken könnte.

Die Bemerkungen am Schluss fließen nicht direkt in die Bewertung ein, da sie sehr unterschiedlich sind, sie sind aber bei der Entscheidung auf jeden Fall zu berücksichtigen (z.B. wenn man immer eine CD braucht um ein Backup zu machen, oder grundlegende Linux-Kenntnisse nötig sind um ein Backup zu erstellen).

8.3 Zentrales Backup

8.3.1 Anforderungen

- Plattformunabhängigkeit
- Umgang mit wechselnden Clients (Laptops)
- Geschwindigkeit
- Plattenplatz
- Einfache Implementierung
- preisgünstig

8.3.2 Bewertungskriterien

- Ist Know-How in Firma vorhanden?
- Werden bestehende Tools verwendet?
- Muss neue HW angeschafft werden?
- Können einzelne Files wiederhergestellt werden?
- Ist die Lösung preisgünstig?

8.3.3 Bewertung

| Produkte / Kriterien (Gewichtung 1-3) | BackupPC | Bacula | Amanda | Arkeia |
|---------------------------------------|---|---|--|---|
| Einzelne Files wiederherstellen (3) | ja | ja | Ohne Komprimierung: ja | Ohne Komprimierung möglich |
| Benutzerfreundlichkeit (3) | User hat fast nichts mit Backup zu tun. Manuell lässt sich ein Backup mit einem Klick starten | Einmal eingerichtet läuft der Daemon selbständig. | Linux- und Shellerfahrung nötig, evtl kann Script Abhilfe schaffen | Einfaches und ansprechendes Java-GUI |
| Backup-Medium (3) | Beliebig, alles was Linux ansprechen kann | Beliebig, alles was Linux ansprechen kann | Tapes | Nein |
| Know-How vorhanden (2) | Ja | Ja, wenig | Nein | Nein |
| Betriebssysteme (2) | Windows, Linux und Mac OS X | Windows, Linux, Mac OS X | Linux & Windows | Linux & Windows |
| Versionisierung | Ja | Ja | Ja | Ja |
| Zentrales Management (1) | Ja | Ja | Ja | Ja |
| Automatisiertes Backup | Ja | Ja | Ja | Ja |
| Preis | Open Source | Open Source | Open source | 999\$ plus jährlich 199\$ |
| Homepage | http:// backuppc.sourceforge.net/ | http://www.bacula.org/ | http://www.amanda.org/ | http://www.arkeia.com/ |
| Bemerkung | Keine SW auf dem Client nötig, alles läuft über das Web | Auf jedem Client muss ein rsync-Daemon laufen. | Nur für Tapes geeignet. Ist deshalb sehr | Komplettpaket für Server und Clients. Relativ |

| | | | | |
|--|----------------------------|---|--|--|
| | und vorhandene Systemtools | Unter Windows nur mit Cygwin betreibbar | eingeschränkt und kann auch keinen schnellen Restore ermöglichen | unflexibles Lizenzmodell, falls mehr als 1TB Daten anfallen muss für jedes zusätzliche halbe Terrabyte 499\$ bezahlt werden. |
|--|----------------------------|---|--|--|

8.3.4

8.3.5 Resultat

Arkeia hat ein grosses Handicap, dass es sehr viel kostet. Wegen der undurchsichtigen Lizenzen, wurde auch nicht sofort klar wofür man wie viel bezahlt. Sicher ist, dass für eine Firmenlösung die angebotenen Speichergrössen lächlich klein sind.

Ein 1TB erreicht man schnell wenn 200 Mitarbeiter alle ihre Daten auf dem Backupserver speichern wollen. Davon abgesehen bietet die Firma ein Komplettpaket, das sich eignet wenn man noch gar keine Backups macht und nun diese in der Firma einführen will. Für eine Client-only Lösung ist dies hingegen eher nicht geeignet.

Armanda ist schon etwas älter wird aber immer noch gepflegt. Die Möglichkeiten sind aber stark begrenzt, da beispielsweise ein Tape als Backup-Device dient und man solche Hardware zuerst anschaffen muss.

Ein Tape bietet leider auch nicht den gewünschten schnellen Restore.

Bacula und BackupPC bieten fast das gleiche an, nur dass Bacula keine Unterstützung für Samba hat und kein GUI besitzt.

Da ein User bekanntlich den Überblick behalten will, und nicht den Umgang mit der Kommandozeile lernen will, ist BackupPC den Vorzug zu geben.

Dank Webinterface muss der Benutzer gar keine Software installieren, lediglich einen Benutzer hinzufügen (Unter Linux SSH-Key-Exchange).

Die Aussicht auf Support innerhalb der Firma hat mich auch überzeugt. Dani Steiner hat mir das Tool bereits gezeigt und ich konnte mir einen ersten Eindruck verschaffen).

8.4 Lokales Backup

8.4.1 Anforderungen

Aufgrund der Mitarbeiter-Umfrage ging hervor, dass doch viele Mitarbeiter immer extern arbeiten und deshalb auch nur lokales Backup machen möchten oder zusätzlich zum zentralen Backup eine lokale Lösung einsetzen wollen.

Die Anforderungen dafür sind folgende:

- Schneller Restore
- Backup über Nacht
- Restore einzelner Files möglich
- Mind. 2 Versionen aufbewahren
- Einfache Benutzerführung

Aus der internen Systemtechnik sind ebenfalls Anforderungen an ein solches System vorhanden:

- Preis/Leistung
- Zentrales Management

IPA: Client Backup Services

- Wenig Plattenverbrauch
- Kompatibilität zu verschlüsselten Disk im Hinblick auf die Einführung von „ProtectDrive“
- Linux und Windows tauglich

8.4.2 Bewertung

| Produkte / Kriterien (Gewichtung 1-3) | Norton Ghost | Acronis True Image | dd | PartImage | Rsync | NTBKP |
|---------------------------------------|---|--|--|---|--|----------------------------------|
| Zeit für Backup (2) | 2h | 2h | 1h 30min | 1h 45min | 45min | 1h 30min |
| Zeit für Restore (3) | 1h 30min | 1h 15min | 1h 30min | 1h 30min | 45min | 1h 15min |
| Einzelne Files wiederherstellen (3) | ja | ja | Ohne Komprimierung: ja | Ohne Komprimierung möglich | ja | ja |
| Speicherplatz (2) | 7.5GB | 7GB | 20GB | 7GB | 7GB | ca. 8GB |
| Benutzerfreundlichkeit (3) | Etwas verwirrende Begriffe, grundsätzlich gut | Gewohnte Umgebung dank BartPE | Linux- und Shellerfahrung nötig, evtl kann Script Abhilfe schaffen | Angenehmes GUI, Linux-Kenntnisse nötig | Linux- und Shellerfahrung nötig, evtl kann Script Abhilfe schaffen | Sehr einfach zu bedienen |
| Backup im Laufenden Betrieb (1) | Nein | Ja | Ja | Nein | Ja | Ja |
| Backup von verschlüsselten Disks (1) | Nein | Ja | Ja | Nein | Ja | Jein (alles ausser System-State) |
| Dateisysteme (2) | NTFS, FAT, ext2, ext3 | NTFS, FAT, ext2, ext3, reiserfs, reiser4, linux swap, HPFS | Alle, da Raw-Image | Alle im Kernel enthaltenen (NTFS ist experimentell) | Alle vom Host unterstützten, da transparenter Zugriff stattfindet | NTFS, FAT |

| | | | | | | |
|--------------------------|--|--|---|--|--|---|
| | | (Apple) | | | | |
| Betriebssysteme (2) | Windows, Linux nur teilweise da Bootloader korrupt wird | Windows, Linux, Apple | betriebsystemunabhängig | Linux, Windows (siehe Dateisysteme) | Linux, Windows, Mac (ab Mac OS X) | Windows |
| Zentrales Management (1) | Nein | Ja, dort lassen sich Backups starten und Status überprüfen | Nein | Nein | Ja, da von Remote machbar, kann man Script schreiben die selbständig Backups auf ein entferntes System machen. | nein |
| Automatisiertes Backup | Nein | Ja | Ja (mit cron) | Ja (mit cron) | Ja (mit cron) | Ja |
| Preis | Lizenzen bereits vorhanden | 50€ je Client (ca. 100-200 Lizenzen erforderlich) | Open source | Open source | Open Source | Integriert in Windows |
| Bemerkung | Bei einer Windows-Installation ist keine CD mehr notwendig | Boot-CD erforderlich | Nicht optimiert, aber plattform unabhängig. Linux-Installation oder Knoppix-Boot CD notwendig. Linux Kenntnisse | Linux Kenntnisse notwendig (Gerätedateien) | Sehr viele Parameter. Linux Kenntnisse notwendig (Gerätedateien) | Leider Windows only, dort aber Top-Lösung |

| | | | | | | |
|--|--|--|------------------------------|--|--|--|
| | | | notwendig (Gerätedateien) | | | |
|--|--|--|------------------------------|--|--|--|

Wichtig: Bei den reinen Daten-Backups müsste man bei einem Totalausfall auch noch die Zeit für das aufsetzen eines neues Betriebssystem anrechen.

8.4.3 Resultat

8.4.3.1 Datenbackup

Um ein reines Datenbackup zu realisieren genügen den Tools der jeweiligen Betriebssysteme. **Unter Windows** ist es ein leichtes sich einen Job mit **NTBKP (NT-Backup)** einzurichten der täglich die wichtigsten Verzeichnisse sichert und auf einen Share ablegt.

Genauso einfach ist das mit **rsync unter Linux**. Man muss sich dafür zwar etwas einlesen oder sonst auf fertige Beispiele zurückgreifen (siehe Anleitung).

8.4.3.2 Backup des Gesamtsystems

Um eine einheitliche Lösung für alle Betriebssysteme zu schaffen (zumindest beim Sichern des Gesamtsystems) ist **Acronis TrueImage die beste Wahl**. Es bietet ein intuitives und vertrautes GUI (für Windows-User) und lässt auch keine Wünsche übrig bei den restlichen Kriterien:

- Zentrales Management
- Storage Server (somit liesse sich gar eine Art Client/Server Architektur aufbauen)
- Task Planer um beispielsweise wöchentlich ein Image zu erstellen
- Image Erstellung im laufenden Betrieb möglich
- Im Hinblick auf die Zukunft ist es auch möglich ein Abbild einer verschlüsselten Disk zu erstellen.

Die Linux-Lösungen eignen sich nur für erfahrene User die ihr System kennen und wissen wie man mit Gerätedateien umgehen muss.

Acronis lässt sich unter Windows installieren und bedarf dann keiner Boot-CD mehr. Linux User müssen auf die Boot-CD zurückgreifen

9 Realisierung

9.1 Aufsetzen der Testumgebung

Bei der Testumgebung ist es sehr wichtig, dass sie auch der Realität entspricht. Der Server ist eine Individual-Installation, bei den Clients hingegen handelt es sich um Standard-Clients gemäss Unternehmensrichtlinien.

Zu Testzwecken wird einige Software und Daten auf die Clients installiert, so dass ein „normaler“ User simuliert werden kann.

9.1.1 Windows-Client

Es handelt sich beim Windows-Client um einen IBM T43 Laptop mit Standardimage. Dieses wird von der internen Systemtechnik bereitgestellt und auch genau so an die Mitarbeiter ausgeliefert. Das Image beinhaltet ein Windows XP mit Standard-

Konfiguration gemäss Unternehmensstandards.

9.1.2 Linux Client

Auf dem Linux-Client (IBM T30) ist ein Open SuSE 10.0 gemäss Unternehmensrichtlinien installiert. Leider gibt es für die Linux-Client kein Image, was die Installation etwas aufwändiger macht. Es handelt sich hier um eine nicht modifizierte Version direkt ab DVD.

9.1.3 Server

Da ich mich bei der Auswertung der Mitarbeiter-Umfrage bereits im Vorfeld Gedanken machen konnte über mögliche Lösungen, war für mich klar, dass ich einen Linux-Server brauchen werde um die zentrale Backup-Lösung BackupPC zu realisieren.

9.1.3.1 Wahl der Distribution

In der Trivadis-Server Landschaft ist die Standard-Distribution für Linux SuSE Enterprise Server 9. Da ich mich aber mit SuSE nicht besonders gut auskenne und ich das fehlerhafte Paketsystem lieber umgehen will, habe ich mich für eine andere Distribution entschieden.

Es ist Gentoo Linux, welches ich persönlich am besten kenne, da ich schon am längsten damit arbeite. Administrieren lässt es sich wie jedes andere Linux-System auch, es hat zusätzlich einfach ein Paketsystem welches sehr ausgereift ist und genau meinen Zwecken dient.

Um keinen Desktop zu installieren muss man dies nicht so umkonfigurieren sondern diesen schlicht nicht installieren. Die Philosophie ist somit etwas anders um ein schlankes System zu bekommen: Man deinstalliert nicht alles was man nicht braucht, sondern installiert genau was man braucht und nur das.

Ich denke für einen Server ist es sehr wichtig, möglich wenig Ballast zu haben, nur wenige ausgewählte Dienste anzubieten und genau den Vorstellungen des Benutzers zu entsprechen. Gentoo unterwirft einem nicht irgendwelchen Distributionseigenheiten, sondern bieten immer mehrere Varianten an.

Der initiale Installationaufwand ist dadurch etwas höher, wird aber durch ein stabiles und angepasstes System belohnt.

9.1.3.2 Installationsanleitung

Da Gentoo keine Distribution ist, die sich einfach ab CD oder DVD installieren lässt muss zuerst ein Grundsystem installiert werden mit Hilfe einer LiveCD.

Für das Grundsystem gibt es eine Anleitung¹, so dass man optimal starten kann.

¹ [Internet, Stand 27.3.06] Gentoo Handbook 2006.0: <http://www.gentoo.org/doc/en/handbook/handbook-x86.xml>

Ich lief nur bei einem Punkt auf, als ich nicht bedacht hatte, dass der Server eigentlich ein RAID-System hat (ich aber nur eine Disk habe). Die Namensgebung des Geräts ist entsprechend anders und der Bootloader „grub“ hat die Festplatte nicht erkannt. Eine Lösung habe ich im Gentoo-Forum² gefunden:

```
# grub --device-map /boot/grub/device.map
(grub) quit
# vi /boot/grub/device.map
Folgende Zeile einfügen: hd0          /dev/ida/c0d0
grub -device-map
(grub) root (hd0,0)
(grub) setup (hd0)
(grub) quit
```

9.1.3.3 Remote-Administration

Um den Server optimal zu administrieren hat der Server eine ILO-Einheit (Insight-Light-Out), mit der sich ihn überwachen und konfigurieren kann. Mit dem Java-Viewer sieht man die Bildschirmausgabe als ob man davor sitzen würde. Der mühsame Weg in den Serverraum bleibt einem so erspart. Ebenfalls lässt er sich ein- und ausschalten. Lediglich um eine CD einzulegen Bedarf es noch eines Gangs zum Server.

Angesprochen wird das ILO über ein eigenes Netzwerkinterface so dass der Zugriff auch bei abgeschaltetem Server gewährt ist.

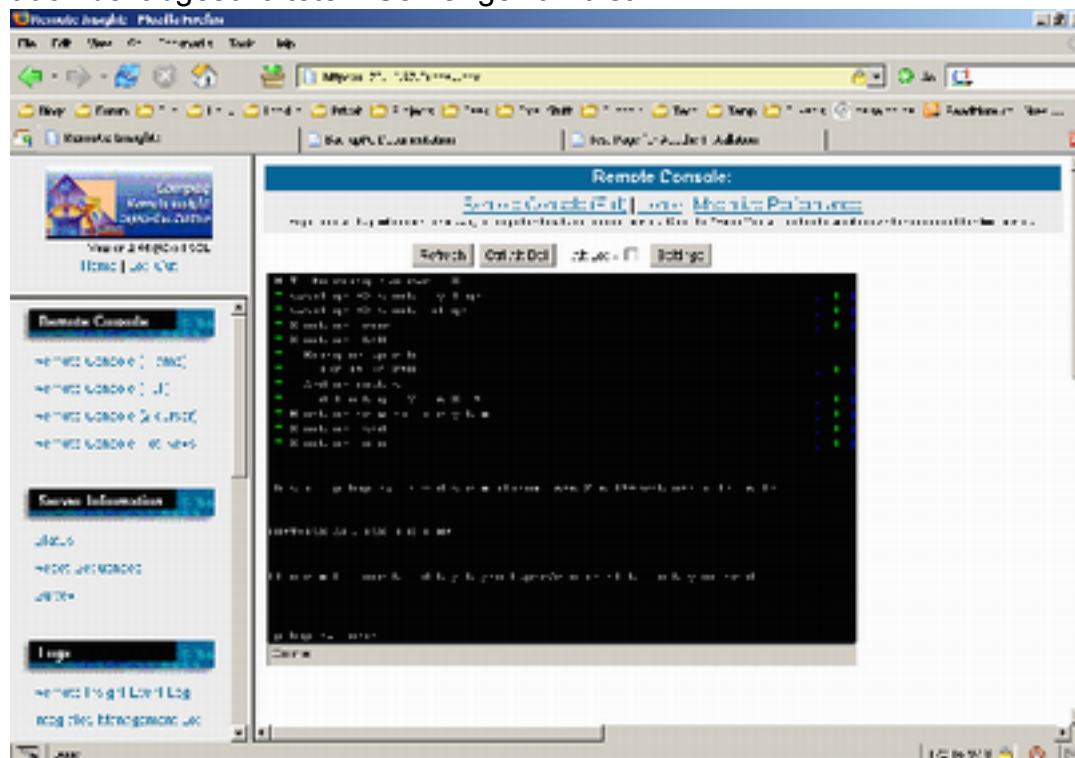
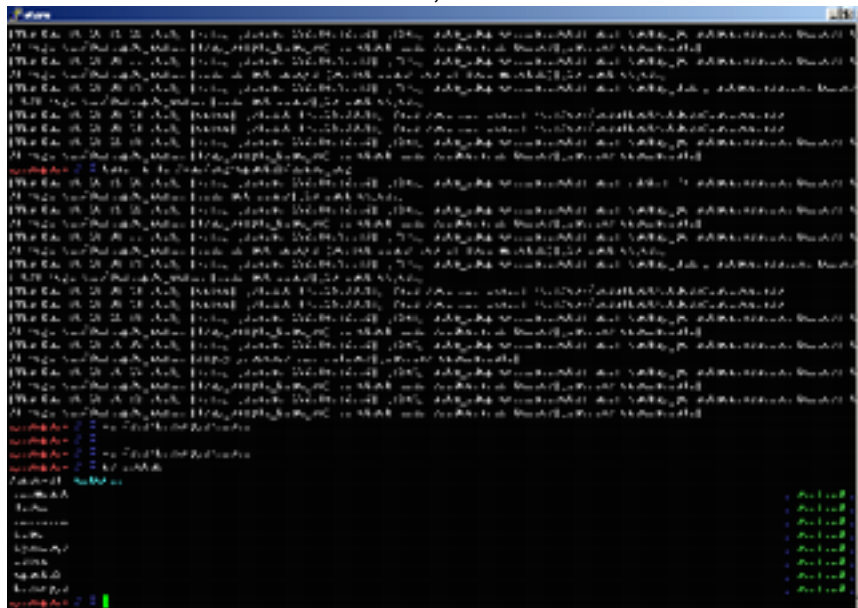


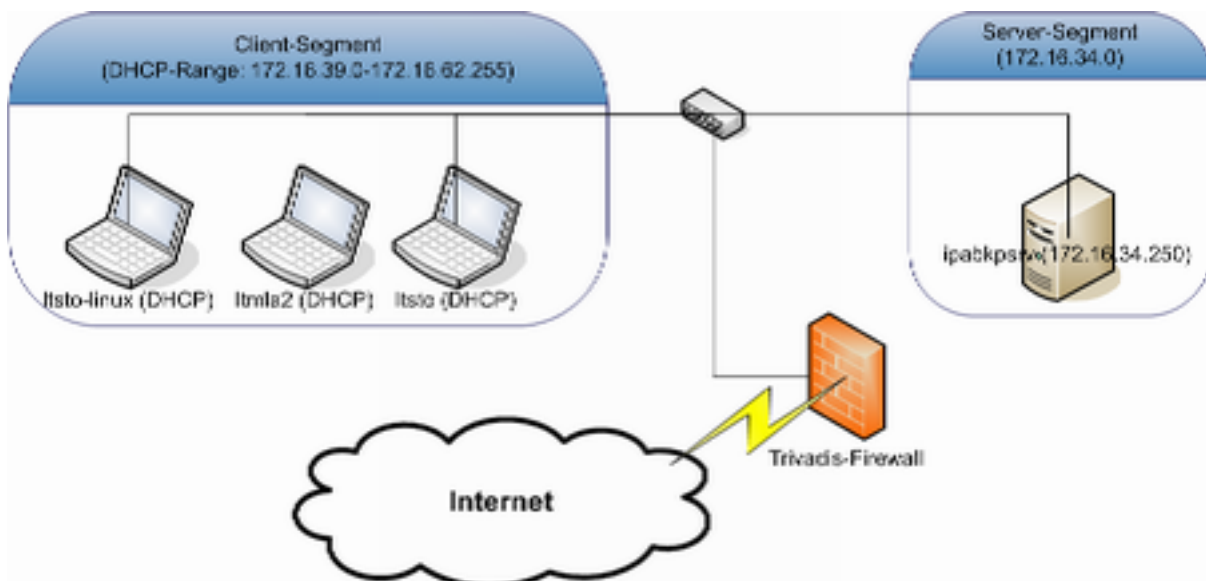
Abbildung 1: Die Remote-Console mit Tastatur- und Maus-Support

² [Internet; Stand: 13.3.06] „Gentoo on a Compaq Proliant DL380 (with SmartArray 5300)“: <http://forums.gentoo.org/viewtopic-t-10380.html>

Das Interface des ILO eignet sich aber nicht besonders gut, um länger daran zu arbeiten. Wenn der Server lief, wickelte ich alles über SSH ab:



9.1.4 Netzwerkschema



9.2 Konfiguration der Testumgebung

9.2.1 Dienste

Folgende Dienste sind auf dem Server installiert:

- SSH (OpenSSH)
- Samba
- Mail (sendmail)
- Cron (fcron)
- Systemlog (sysklogd)

- BackupPC
- Webserver (Apache)

Um den Server komfortabel betreiben zu können, sollten die obengenannten Dienste in einem Runlevel laufen, das bedeutet, dass sie beim booten automatisch gestartet werden. Für selbst installierte Dienste bietet sich das „default“-Runlevel an, das am Schluss startet (vor der grafischen Oberfläche). Dies geschieht – jeweils für jeden Dienst – so:

```
ipabkpsrv / # rc-update add <dienstname> default
```

9.2.1.1 Apache2 mit mod_perl und mod_auth_ldap

Um unter Gentoo ein Paket zu installieren muss man zuerst alle möglich Optionen prüfen, um am Schluss das Paket mit Unterstützung für alles gewünschte zu erhalten (LDAP zum Beispiel).

Dies geschieht mittels der Datei /etc/portage/package.use:

```
net-www/apache mpm-prefork doc ldap
```

Dann kann man prüfen ob alles aktiviert ist, was man braucht und schon wird die Software heruntergeladen, die Quelltexte ausgepackt, das Ganze kompiliert und schliesslich installiert:

```
ipabkpsrv / # emerge -pv apache

These are the packages that I would merge, in order:

Calculating dependencies ...done!
[ebuild R ] net-www/apache-2.0.55-r1 +apache2 -debug +doc +ldap -
mpm-leader -mpm-peruser +mpm-prefork -mpm-threadpool -mpm-worker -no-
suexec (-selinux) +ssl -static-modules -threads 4684 kB
```

SSL und LDAP sind aktiviert, das bedeutet, dass mod_ldap, mod_auth_ldap und mod_ssl automatisch mitkompiliert werden.

Zur Ausführung des CGI-Perl Script braucht es nun noch mod_perl:

```
ipabkpsrv / # emerge mod_perl
```

Ist auch das geschafft, muss Apache noch entsprechend konfiguriert werden.

In der Datei /etc/conf.d/apache2:

```
APACHE2_OPTS="-D DEFAULT_VHOST -D PERL -D SSL -D SSL_DEFAULT_VHOST -D
LDAP -D AUTH_LDAP -D INFO"
```

-D steht für „define“ und setzt diese Variablen auf „true“, in den Konfigurationsfiles kann dann jeweils mit <ifDefine LDAP> usw. auf diese geprüft werden. Wichtig für BackupPC ist hier PERL (mod_perl wird aktiviert), LDAP (aktiviert mod_ldap), AUTH_LDAP (aktiviert mod_auth_ldap) und INFO (zuständig für ausführlichere Debugmeldungen)

und die Test-Seiten auf dem Server).

In der Datei `/etc/apache2/modules.d/46_mod_ldap.conf` (dieses File wird beim kompilieren mit der LDAP-Option automatisch erstellt und muss nur noch ergänzt werden):

```

<IfModule util_ldap.c>

    LDAPSharedCacheSize 200000
    LDAPCacheEntries 1024
    LDAPCacheTTL 600
    LDAPOpCacheEntries 1024
    LDAPOpCacheTTL 600
    LDAPTrustedCA /etc/apache2/ssl/twe.crt
    LDAPTrustedCAType BASE64_FILE

    <Location /ldap-status>
        SetHandler ldap-status
        Order deny,allow
        Deny from all
        Allow from 127.0.0.1
    </Location>

</IfModule>

# BackupPC Configuration
<Location /cgi-bin/BackupPC_Admin>
    AuthType Basic
    AuthName "BackupPC Login"
    AuthLDAPAuthoritative on
    AuthLDAPRemoteUserIsDN off
    AuthLDAPDereferenceAliases never

    AuthLDAPURL ldaps://donar.trivadis.com:636/dc=trivadis,dc=com?
uid?sub?
    #AuthLDAPURL ldap://donar.trivadis.com:389/dc=trivadis,dc=com?
uid?sub?

    require valid-user
</Location>

```

Diese Einstellungen geben ein Server-Zertifikat an, welches für SSL benötigt wird (LDAPTrustedCA).

Das Location-Tag zeigt an für welchen Pfad diese Authentifizierung gilt.

Die Direktive `AuthLDAPURL` gibt an wo der Server Username/Passwort prüfen soll. Das Präfix `ldaps://` stellt sicher, dass dies mit LDAP over SSL läuft (verschlüsselte Verbindung zum LDAP-Server).

9.2.1.2 Samba einrichten

Auf dem Server dient Samba nur als Helfer. Es werden keinerlei Shares angeboten und auch keine Shares gemountet (jedenfalls nicht fix). Zum einen braucht BackupPC das Programm `smbclient` um Daten mit den Clients auszutauschen. Zum anderen dient das Tool `nmblookup` eine Suche nach NetBIOS-Namen, auf diese Art werden die meisten Clients gefunden, da es sich um ein DHCP-Netz handelt und die

Clients normalerweise nicht auf dem DNS eingetragen sind.

NetBIOS ist ein stabiler Workaround, da der Trivadis DHCP-Server leider keine Namen dynamisch auflösen kann. Der einzige Wehrmutstropfen ist, dass ein Linux-Client mit grösster Wahrscheinlichkeit einen laufenden Samba-Server benötigt, um den NetBIOS-Namen im Netz bekannt zu machen.

Um den Server nicht einer unnötigen Gefahr auszusetzen, sollte in der Datei `/etc/samba/smb.conf` alle Shares auskommentiert werden, da diese nicht benötigt werden. Auch die Freigabe der Drucker sollte sicherheitshalber deaktiviert werden.

9.2.2 SSH und Key-Exchange

Um SSH per Script laufen zu lassen ist es nicht sehr klug den Login im Klartext in das Script zu schreiben. Am besten erledigt man das über die sogenannten „authorized keys“. Es sind RSA oder DSA-Keys die auf dem Client kreiert (Private- und Public-Key) werden und dann wird der Public-Key auf dem Server hinterlegt. Kommt nun ein Login von einem vordefinierten Host, wird dieser ohne Passwort Abfrage auf das System gelassen.

Client:

```
$ ssh-keygen
```

```
ssh-keygen -t dsa
```

Generating public/private dsa key pair.

Enter file in which to save the key (/home/backuppc/.ssh/id_dsa):

Enter passphrase (empty for no passphrase):

Enter same passphrase again:

Your identification has been saved in /home/backuppc/.ssh/id_dsa.

Your public key has been saved in (/home/backuppc/.ssh/id_dsa.pub).

The key fingerprint is:

```
d4:f1:97:8e:3e:c4:50:fb:67:e0:40:aa:6f:b2:d4:33 backuppc@ipabkpsrv
```

Wichtig ist, dass der Key mit dem User erstellt wird, mit dem sich das Script dann verbinden will. Das File nun auf den Server kopieren:

```
scp /home/backuppc/.ssh/id_dsa.pub root@ltsto-linux:/root/backuppc_dsa.pub
```

Server:

```
cat backuppc_dsa.pub >> /root/.ssh/authorized_keys2
```

Der User „backuppc“ hat nun das Recht sich auf dem Server mit dem Benutzer root ohne Passwort einzuloggen.

9.2.3 Integration ins Trivadis Backupkonzept

Auf dem Backup-Server tvdbackup habe ich ein Verzeichnis für meinen Server anlegen lassen. Darin habe ich Platz den Server zu sichern.

Der Share /backup ist auf dem tvdbackup Server via Samba gemountet.

Dies mache ich über folgendes dar Script³:

```

# run this script to create an archive using the following dar command.
dar=`which dar`
echo $dar|grep -Eq 'dar$'
if [ $? -ne 0 ]; then
    echo -e "Error:\tIs the dar binary installed? Or is it not in the
PATH?\n"
    exit 2
fi
base="/"
prefix="/backup"
host="ipabkpsrv"
exclude="dev/pts mnt/* backup proc sys usr/portage var/tmp"
opts="-v -c ${prefix}/${host}-full -R ${base} -s 2147483648 -p -D -y -m
150"

ex=""
for e in `echo ${exclude}`; do
    if [ "$ex" = "" ]; then
        ex="-P $e"
    else
        ex="${ex} -P $e"
    fi
done

echo "$dar ${opts} ${ex}"
$dar ${opts} ${ex}

```

Das Script prüft zuerst ob dar vorhanden ist, falls nicht wird eine Fehlermeldung ausgegeben. Die Verzeichnisse bei exclude werden nicht gesichert, sonst alles was sich unterhalb von base befindet (hier also /).

Das inkrementelle Gegenstück sieht so aus:

```

#!/bin/bash

# Run this script to create an archive using the following dar command.

# because this is an incremental-script we use a paramater to speciy
which number it is (good for cron) added by sto
number=$1

dar=`which dar`
echo $dar|grep -Eq 'dar$'
if [ $? -ne 0 ]; then
    echo -e "Error:\tIs the dar binary installed? Or is it not in the
PATH?\n"
    exit 2
fi
host="ipabkpsrv"
prefix="/backup"
base="/"

```

³ Die Script-Vorlage wurde mir von Dani Steiner (Trivadis-Consultant) zur Verfügung gestellt.

```

exclude="dev/pts mnt/* backup proc sys usr/portage var/tmp"
opts="-v -c ${prefix}/${host}-incr-${number} -R ${base} -A ${prefix}/
${host}-full -w -s 2147483648 -p -D -y -m 150"

ex=""
for e in `echo ${exclude}`; do
    if [ "$ex" = "" ]; then
        ex="-P $e"
    else
        ex="${ex} -P $e"
    fi
done
echo "$dar ${opts} ${ex}"
$dar ${opts} ${ex}

```

Der Parameter `-A` gibt an zu welchem Full das inkrementell die Unterschiede speichern soll. Via Parameter wird die Nummer des Incrementals angehängt (siehe unten).

Um die beiden Script regelmässig zu starten wird `cron` verwendet:

```

ipabkpsrv / # crontab -e
27 1 * * 0 /root/ipabkpsrv-full_backup.sh
27 1 * * 1 /root/ipabkpsrv-incr_backup.sh 01
27 1 * * 2 /root/ipabkpsrv-incr_backup.sh 02
27 1 * * 3 /root/ipabkpsrv-incr_backup.sh 03
27 1 * * 4 /root/ipabkpsrv-incr_backup.sh 04
27 1 * * 5 /root/ipabkpsrv-incr_backup.sh 05
27 1 * * 6 /root/ipabkpsrv-incr_backup.sh 06

```

Der Backup-Server selbst sichert jede Woche die Daten auf Tape, so dass eine genügende Sicherheit besteht.

9.3 BackupPC

BackupPC ist eine CGI-basierte (Perl) Weblösung um Backups an zentraler Stelle zu erstellen. Dies geschieht über zwei Wege:

- Scheduling (definierte Zeiträume)
- On-Demand (der User kann das Backup selbständig auslösen)

9.3.1 Installation

Die Installation von BackupPC verläuft genau so einfach wie alle Installation ein simples:

```

emerge backuppc

```

genügt.

Dank dem Tool `webapp-config` wird BackupPC automatisch als eine Webapplikation eingerichtet, die entsprechenden Verzeichnisse und User werden erstellt.

9.3.1.1 Files und User

Script: `/var/www/localhost/cgi-bin/BackupPC_Admin`

IPA: Client Backup Services

Bilder/CSS: /var/www/localhost/htdocs/backuppc

Platz für Backups: /var/lib/backuppc/

Konfiguration: /etc/backuppc

User: backuppc:x:101:408:BackupPC user:/home/backuppc:/bin/bash

Der User ist einfach ein Eintrag im File `/etc/passwd`. Dies wurde bereits um ein gültiges Home-Verzeichnis und eine Shell erweitert, da dies in der Standardeinstellung fehlt, wir es aber um SSH zu verwenden dringend brauchen.

9.3.2 Konfigurationsfiles

Das Konfigurationssystem von BackupPC ist überraschend einfach. Das File ist ein ausführbares Perl-Script, das somit auch das einbinden weiterer Files zulässt. Jede Option hat einen erklärenden Text dazu und somit lässt sich ein Grossteil ohne einen Blick ins Handbuch konfigurieren.

Um die verschiedenen Konzepte zu realisieren braucht es auch mehrere Konfigurationsfiles. Das File `/etc/backuppc/config.pl` ist das Hauptkonfigurationsscript und kommt zum Einsatz wenn nichts anderes angegeben ist. Für die Linux und Windows-Varainten habe ich jeweils ein File erstellt, sowie für die Minimal-Variante die allerdings unabhängig funktioniert.

Um eine Per-PC Konfiguration zu realisieren muss eine Config-File in den jeweiligen Ordner des Clients kopiert oder mit Symlinks verlinkt werden (`/var/lib/backuppc/pc/<hostname>/config.pl`).

9.3.3 Host finden

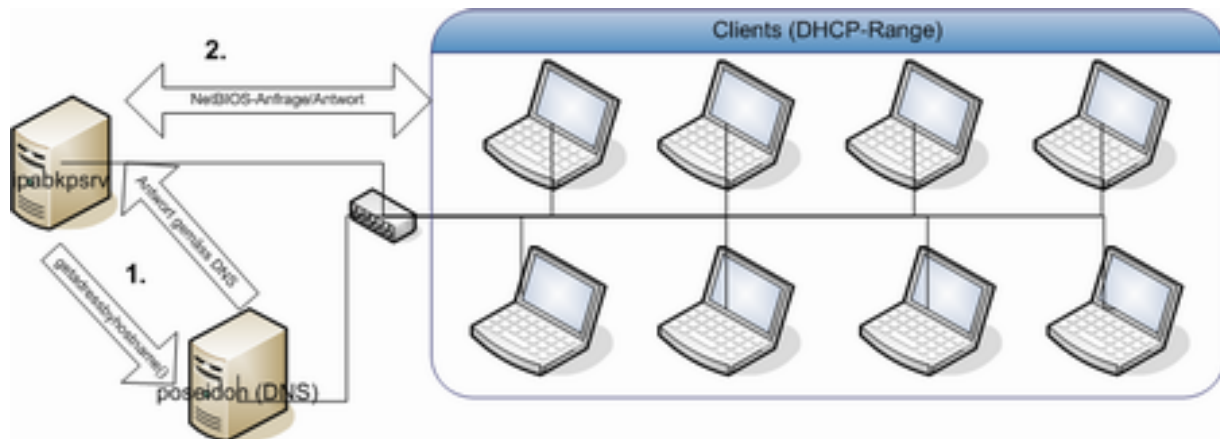
Host werden über zwei Mechanismen gefunden und setzen einen Eintrag im BackupPC-Host File voraus (`/etc/backuppc/hosts`):

```

-----
Host      dhcp      user      moreUsers
localhost 0         backuppc
ltsto     0         sto
ltsto-linux 0       sto      backup_dummy
ltipasto  0         backup_dummy sto
-----

```

Ist der Host dort eingetragen versucht BackupPC mit der Perl-Methode `gethostbyname()` die IP-Adresse zu finden. Dies funktioniert nur bei Hosts die auf dem DNS eingetragen sind, was bei den wenigsten der Fall ist. Viel eher funktioniert eine NetBIOS-Abfrage über den Systembefehl `nmblookup`.



Windows Clients sprechen untereinander häufig mit NetBIOS und die Namen sind auch bekannt im Netzwerk. Da es intern keinen WINS-Server gibt, muss ich einen laufenden Samba-Server für die Linux-Clients voraussetzen, die einen korrekten NetBIOS-Name eingetragen haben.

Ist ein Client als DHCP konfiguriert ist es auch wichtig, dass er sich im vorkonfigurierten DHCP-Bereich befindet, nur so wird er zugelassen. Über diesen Bereich lässt sich auch steuern, dass nicht irrtümlich ein Server ein Backup starten kann. Bei unserer sauberen Netzsegmentierung kann man diesen Angaben auch Glauben schenken. Ebenfalls möglich wird das ausschliessen von bestimmten Lokationen, da diese vielleicht selbst einen Backup-Server betreiben. Die Datenübertragung über WAN sollte ja nach Möglichkeit geschont werden.

Leider ist die Angabe von DHCP-Ranges im Konfigurationsfile mühsam, da sich nur Class-C Netze angeben lassen, wir aber einen Range haben, der sich über die Grenzen eines Class-C Netz hinausbewegt, deshalb wären dort für eine einzige Lokation mehr als 20 Einträge nötig.

In der BackupPC-Dokumentation wird empfohlen gar keine DHCP-Flags zu setzen da sich der Suchprozess nur verlangsamt. Dann sollte aber jedenfalls sichergestellt sein, das der NetBIOS-Name aufgelöst werden kann.

9.3.4 Limitationen

9.3.4.1 Gelockte Files

Da das Backup im laufenden Betrieb gemacht wird, gibt es klar Limitationen. Files die offen sind, nicht vom Betriebssystem gelockt und können nicht gesichert werden. Auch Outlook-Datendateien (.pst) können nicht gesichert werden wenn Outlook läuft. Systemdateien die gerade vom Betriebssystem gebraucht werden und natürlich auch der Swap-Bereich oder der Kernel, können nicht gesichert werden.

9.3.4.2 Filesystem des Servers

Bei der Speicherung auf dem Server gibt es auch noch Limitationen vom Filesystem her. Bei 31'999 Links auf dasselbe File ist die maximale Anzahl erreicht (BackupPC macht intensiv Gebrauch von sogenannten Hardlinks). Um die vielen Files auf

einer grossen Installation zu verwalten, empfiehlt BackupPC reiserfs, das mit vielen Dateien besser umgehen kann, aber nicht so performant ist.

Ich habe für die Serverinstallation ext3 als Filesystem genommen, da es sehr schnell ist und ich keine grosse Installation habe (nur 3 Clients auf einer 20GB Festplatte).

9.3.4.3 Grosse Dateien

Da Perl mit „largefiles“ kompiliert wurde unterstützt gibt es von der Seite keine Einschränkung. Mit SMB (Samba) gilt eine maximale Grösse von 4GB (je nach Version sogar nur 2GB). Rsync hat keine solche Einschränkung, ausser es läuft mit cygwin unter Windows.

Für Linux-User gilt als das Limit von vom Filesystem ext3, das LFS unterstützt und eine maximale Filegrösse von 2 TiB⁴ hat.

9.3.4.4 Dateiattribute

Dateiattribute die über die Standard-Attribute von Unix ausgehen (Read-Write-Execute, jeweils auf Owner, Group und World) können mit BackupPC leider nicht gespeichert werden.

Jegliche Windows-ACL (Access Control List) können nicht gespeichert werden.

9.3.5 Datenübertragung

Um Files von Clients zu holen und diese dann zu sichern bietet BackupPC mehrere Varianten an:

- Rsync (geänderte Files übertragen per SSH-Tunnel kopieren)
- Samba (Files über einen Windows-Share kopieren)
- Tar (mit tar die Files archivieren und per SSH-Tunnel kopieren)
- Rsyncd (direkt bei einem laufenden Rsync-Daemon anmelden und Files holen)

Für Windows-User kommt praktisch nur Samba in Frage, ausser die lassen einen rsyncd via Cygwin laufen, somit ist klar, dass Samba unterstützt werden muss.

Für Linux ist rsync klar die beste Lösung, da nur geänderte Files übertragen werden und nicht jeder Client einen Daemon laufen lassen muss. Die Übertragung der SSH bietet auch grossmöglichen Schutz.

9.3.5.1 Rsync

Rsync bietet eine Unzahl an Parametern die teilweise schon voreingestellt sind. In meiner Konfiguration habe ich noch zwei hinzugefügt, wobei es immer dem User überlassen ist, ob er die Option will oder nicht.

Dass Rsync ohne probleme läuft und nicht versucht nicht benötigte Daten zu lesen lohnt sich auf jedenfall ein das ausschliessen von /dev und /proc. Wer es noch

⁴ Binäre Schreibweise: <http://www.pcguides.com/intro/fun/bindec.htm>

besser machen will, der gibt alle Mount-Points seiner verschiedenen Partition an, und verwendet dann „one-file-system“. Somit liest rsync innerhalb des Baums nur soweit bis eine Partition fertig ist.

```

$Conf{XferMethod} = 'rsync';
$Conf{RsyncShareName} = ['/'];
$Conf{RsyncArgs} = [
    # Do not edit these!
    #
    '--numeric-ids',
    '--perms',
    '--owner',
    '--group',
    '--devices',
    '--links',
    '--times',
    '--block-size=2048',
    '--recursive',
    #
    # Add additional arguments here
    #
    '--exclude','/proc',
    '--exclude','/dev',
    '--one-file-system',
];
$Conf{RsyncClientCmd} = '$sshPath -q -x -l root $hostIP $rsyncPath
$argList+';
#      $host          Name des Clients
#      $hostIP        IP des Clients
#      $shareName     Share-Name den man sichert möchte
#      $rsyncPath     absolute Pfadangabe zu rsync
#      $sshPath       absolute Pfadangabe zu ssh
#      $argList       die oben erstellte Argumentliste
#
#

```

Der RsyncClientCommand definiert genau das ausgeführte Kommando auf dem Client. Das bedeutet dort kann man auch Anpassungen vornehmen wegen anderen Benutzernamen u.ä.

Die dort verwendeten Variablen werden zur Laufzeit aufgelöst wie oben beschrieben. Abweichend von der Orgianlkonfiguration ist die Verwendung von \$hostIP. Dies ist so eingestellt, da zwar mit `nmblookup` zu einem Hostname die korrekte IP ermittelt werden kann, jedoch eine Kommunikation direkt über den Hostname ist nicht möglich. Deshalb soll dort mit der IP gearbeitet werden (dies habe ich herausgefunden, da ich ständig Verbindungsfehler bekommen habe; es ist vor allem ein Linux-Problem, da NetBIOS nicht direkt einen Eintrag im `/etc/hosts`-File auslöst.

9.3.5.2 SMB (Samba)

Samba ist die Standardeinstellung für Windows (smb ist das Protokoll für die Windows-Freigaben, Microsoft nennt es CIFS [Common Internet FileSystem]).

Unter Linux lässt sich auch ein SMB-Share einrichten, dazu ist ein Samba-Server notwendig (bei SuSE bereits vorinstalliert).

Samba ist klar langsamer als rsync, wie meine Tests zeigen. Samba hat aber auch einen Parameter um ein inkrementelles Backup zu machen, somit werden unveränderte Files verworfen, leider geschieht dies nicht schon auf dem Client was unnötig Datenverkehr verursacht. Um es den Benutzern so einfach wie möglich zu machen habe ich auf dem Active Directory einen User erstellen lassen (backup_pc), den sie als lokalen Administrator einrichten müssen wenn sie Backup via Samba machen wollen.

```

$Conf{XferMethod} = 'smb';
$Conf{SmbShareName} = 'backup';

$Conf{SmbShareUserName} = 'backup_pc';
# aus Sicherheitsgründen durch * ersetzt
$Conf{SmbSharePasswd} = '*****';

$Conf{SmbClientFullCmd} = '$smbClientPath \\\\$host\\\$shareName'
    . ' $I_option -U $userName -E -N -d 1'
    . ' -c tarcode\\ full -Tc$X_option - $fileList';

$Conf{SmbClientIncrCmd} = '$smbClientPath \\\\$host\\\$shareName'
    . ' $I_option -U $userName -E -N -d 1'
    . ' -c tarcode\\ full -TcN$X_option $timeStampFile -
$fileList';

```

Beim inkrementellen Befehl wird der Timestamp (Zeitstempel, Zeit der letzten Änderung) noch beachtet. Die verwendeten Variablen werden wiederum zur Laufzeit gefüllt. Die angegebenen Parameter entsprechen den BackupPC-Vorgaben.

9.3.6 Versionisierung

BackupPC bietet verschiedene Funktionen um Backups zu Versionisieren. Man kann zyklisch sogenannte Full-Backups machen, die unabhängig von allem alle Files im angegebenen Share (egal ob rsync oder smb) sichert. Zwischen zwei Full-Backups liegen die „Incrementals“, die jeweils nur die Änderung zum letzten Full- oder Incremental-Backup sichern.

```

$Conf{FullPeriod} = 4.97;
$Conf{IncrPeriod} = 0.97;

```

9.3.6.1 \$Conf(FullPeriod)

\$Conf(FullPeriod) bestimmt die Zeit, in der Full Backups erstellt werden, der Wert sollte ein bisschen unterhalb der tatsächlichen Zahl sein (also 5) da die Zeit die ein Backup braucht, und die Zeit die der Cron-Job braucht um das Backup anzustossen auch in die effektive Zeit einfließen.

9.3.6.2 \$Conf(IncrPeriod)

`$Conf{IncrPeriod}` ist analog dasselbe für die Incremental-Backups, die hier täglich eingestellt sind.

9.3.7 Zeitmanagement

Im Config-File lässt sich relativ genau festlegen, wie viele Backups von welcher Zeit behalten werden und wann Backups ausgeführt werden bzw. eben nicht ausgeführt werden.

```

# Schedule für Cron
$Conf{WakeUpSchedule} = [1..23];

# Zeitmanagement für Full Backups
$Conf{FullKeepCnt} = [3, 0, 2, 0, 1, 1];
$Conf{FullKeepCntMin} = 7;
$Conf{FullAgeMax} = 365;

# Zeitmanagement für Incremental-Backups
$Conf{IncrKeepCnt} = 10;
$Conf{IncrKeepCntMin} = 1;
$Conf{IncrAgeMax} = 60;

# Blackout Zeiten zur Minderung der Netzlast
$Conf{BlackoutBadPingLimit} = 2;
$Conf{BlackoutGoodCnt} = 8;
$Conf{BlackoutPeriods} = [
  {
    hourBegin => 8.0,
    hourEnd => 12.0,
    weekDays => [1, 2, 3, 4, 5],
  },
  {
    hourBegin => 13.0,
    hourEnd => 17.0,
    weekDays => [1, 2, 3, 4, 5],
  },
];

```

9.3.7.1 Schedule (Zeitplan)

`$Conf{WakeUpSchedule}` definiert den Cron-Job der Backups prüft. Die Einstellung `[1..23]` bedeutet, dass jede Stunde ausser Mitternacht geprüft werden soll, ob Clients bereit zum Backup sind. Je nach System wird mit 24 und 0 falsch umgegangen, deshalb empfiehlt BackupPC diese Einstellung für eine stündliche Überprüfung den ganzen Tag.

9.3.7.2 Full-Backups

`$Conf{FullKeepCnt}` ist eine der spannendsten Optionen von BackupPC. Ein Backup soll ja eine möglich grosse Zeitspanne abdecken und dabei wenig Speicherplatz belegen. Dies ist scheinbar widersprüchlich und erfordert einiges an Kompromissen. Der Wert legt fest wie viele Backups behalten werden. Setzt man ihn einfach auf eine Zahl wie beispielsweise 5, werden die 5 letzten Full Backups behalten. Gibt man

dagegen ein Array von Werten an wie in meiner Konfiguration, also [3, 0, 2, 0, 1, 1], so kann man ein sogenanntes exponentielles Backup realisieren. Die Werte werden jeweils $2^{\langle \text{Position} \rangle} * \$\text{Conf}\{\text{FullPeriod}\}$ gerechnet.

Bei der obigen Konfiguration sähe das so aus:

$3 * 2^0 * 4.97$ = die 3 aktuellsten Backups (ca. 0-15 Tage zurück)

$0 * 2^1 * 4.97$ = kein Backup im Bereich 10 Tage (ca. 10-20 Tage zurück)

$2 * 2^2 * 4.97$ = zwei Backups im Bereich 20 Tage (ca. 20-40 Tage zurück)

$0 * 2^3 * 4.97$ = kein Backup im Bereich 40 Tage (ca. 1 Monate 10 Tage zurück)

$1 * 2^4 * 4.97$ = ein Backup im Bereich 80 Tage (ca. 2½ Monate zurück)

$1 * 2^5 * 4.97$ = ein Backup im Bereich 160 Tage (ca. 5 Monate zurück)

So kann man eine relativ grosse Zeitspanne einfach abdecken.

$\$\text{Conf}\{\text{FullAgeMax}\}$ definiert eine Zeit in Tagen, die ein Backup maximal alt sein darf, sonst wird es gelöscht. Es werden aber mindestens $\$\text{Conf}\{\text{FullKeepCntMin}\}$ Backups behalten, egal wie alt sie sind.

Die 7 definierten sind die einzigen die sicher behalten werden sollen. Falls der User aber selbständig Backups macht, können diese bis zu 1 Jahr als sein.

9.3.7.3 Incremental-Backups

Incremental Backups werden nur als Zwischenstufen von zwei Full-Backups gebraucht, deshalb müssen sie auch nicht so lang gespeichert bleiben. $\$\text{Conf}\{\text{IncrKeepCnt}\}$ definiert wie viele genau gespeichert werden, mit 15 macht das 3 Full Backups die aus der aktuellen Zeit stammen (dies definiert $\$\text{Conf}\{\text{IncrAgeMax}\}$).

Es muss aber nur mindestens 5 vorhanden sein, um einen Stand zwischen den letzten zwei Full Backups zu sehen ($\$\text{Conf}\{\text{IncrKeepCntMin}\}$).

9.3.7.4 Blackout-Zeiten

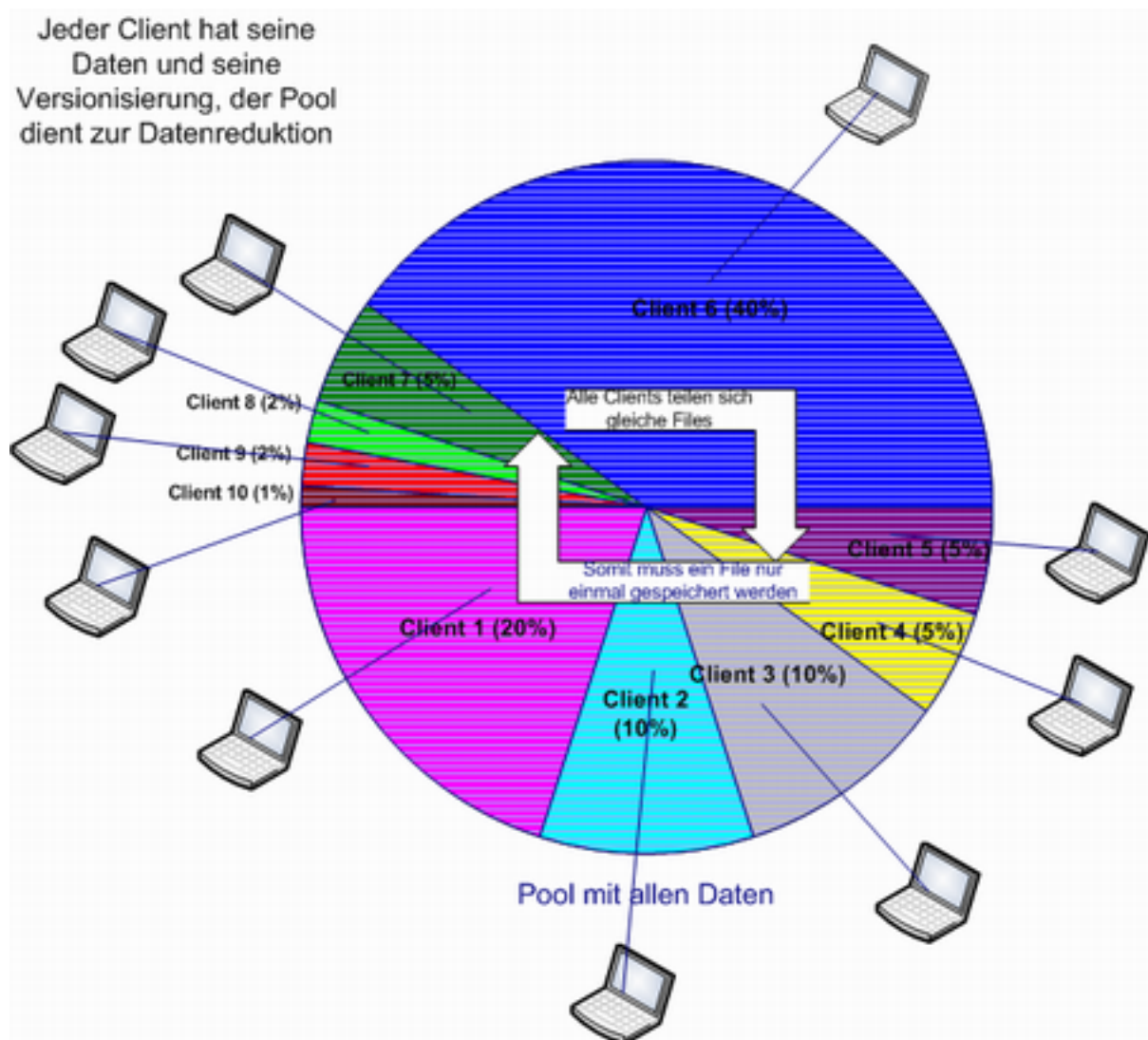
Mit den Blackout-Zeiten haben die Entwickler vom BackupPC ein gefährliches Werkzeug geschaffen. Es ist sehr leicht missverständlich beschrieben, was diese genau machen. Meine Idee war, dass Clients die sich nicht sichern lassen, während der Blackout-Zeiten nicht zusätzlich den Server stören, indem er sie die ganze Zeit überprüfen muss. Also habe ich die normalen Bürozeiten eingetragen.

Die Idee hinter den Blackout-Zeiten ist allerdings eine ganz andere: Nämlich, dass Server nicht die Clients stören. Da sich mit BackupPC viele Geräte (egal ob Client oder Server) sichern lassen, sollen die Server die nicht so netzaktiven Zeiten in der Nacht verwenden.

BackupPC verwendet dazu den Mechanismus der „aufeinanderfolgenden Pings“ (consecutive pings). Gibt ein Client – je nach Einstellung – 7mal Antwort, gilt er als aktiv. Ist in der Konfiguration eine Blackout-Time aktiviert, so wird er während dieser Zeit nicht gesichert.

Da bei meiner Installation aber keine Server vorkommen, habe ich diese Option deaktiviert, da die Clients ja genau während der Büro-Zeite (sprich wenn die Computer laufen) gesichert werden sollen. Sollten später Server dazu kommen, müsste für sie ein eigenes Konfiguration-File erstellt werden und dort diese Blackout-Time eingestellt werden.

9.3.8 Pooling



BackupPC nutzt eine geniale Technik um Files zu speichern. Da ein Backup-System meist unter Platzmangel leidet oder man schlicht und einfach den Platz optimal nutzen will, bietet BackupPC eine Reihe schonender Techniken mit.

Wenn man ein Backup macht fallen immer auch statische Files in die zu sichernden Daten. Ändert sich nun das File nicht mehr, wird es ja bekanntlich bei einem Incremental nicht mehr gespeichert. So ähnlich funktioniert das Pooling einfach auf globaler Ebene.

Will nun ein Laptop ein File speichern, das es bereits gibt, erstellt BackupPC schlicht einen Hardlink auf das File, das im Pool liegt. In den Pool kommen grundsätzlich alle Daten von allen Backups, unabhängig von Betriebssystem, Berechtigung oder Transfermethode.

Das klassische Beispiel ist ein Mail mit einem 10MB Attachment, dass an 10 Leute verschickt wird die dann Backups machen.

BackupPC speichert dieses Attachment nur einmal, und verweist immer auf dieses File. Hat man einmal ein Standard Windows XP und ein SuSE Linux 10.0 gesichert werde viele solche statischen Files anfallen die bei jeder Installation gleich sind, so lässt sich der verbrauchte Plattenplatz drastisch verringern.

9.3.9 Kompression

Die Dokumentation empfiehlt unbedingt die Kompression eingeschaltet zu lassen. Als Kompressions-Methode kommt GZip zum Zug, dass als sehr schnell gilt dafür etwas grössere Files erstellt. GZip kann man mit dem Parameter `-0` (keine Kompression, sehr schnell) bis `-9` (hohe Kompression, langsam) wählen. BackupPC empfiehlt bei grossen Systemen `-3`, ich habe `-6` gewählt und bin damit gut gefahren (hat auch die Erfahrung im Zusammenhang mit `dd` (siehe 7.3 Lokales Backup) gezeigt, welches ich für die lokale Backup-Lösung intensiv getestet habe).

9.3.10 Quota (Speicherplatzbeschränkung)

BackupPC bietet keine Möglichkeit den Platz pro User zu beschränken. Daher können nur empfehlungen herausgegeben werden. Der Disk-Space definiert im Endeffekt den verfügbaren Speicherplatz.

Das einzige Quota das man setzen könnte, das das für den Systembenutzer `backuppc`, unter dem BackupPC läuft. Auf diesem Weg kann auch eine Warnung ausgelöst werden und mehr Speicherplatz eingesetzt werden. Aus diesen Gründen ist es sehr empfehlenswert BackupPC auf einem Server mit RAID-Untersützung zu installieren, so dass bei Bedarf auf einfachste Weise den Speicherplatz vergrössert werden kann.

9.3.11 Konzepte

Um für alle ein angepasstes Backup zu ermöglichen und doch nicht für jeden eine Individual-Lösung einrichten zu müssen, habe ich jeweils für Windows und Linux zwei Varianten erstellt. Das eine ist ein Full-Backup und das andere ein Backup eines Shares (der theoretisch auch die ganze Platte widerspiegeln könnte)

9.3.11.1 Linux-Varianten

Linux-User bilden in der Trivadis einen Kreis von Poweruser. Das bedeutet sie kennen ihr System und wissen meist, was sie backupen wollen und was nicht. Um sie optimal zu unterstützen, habe ich mir mehrere Wege ausgedacht, wie sich ein Linux-System mit BackupPC backupen lässt.

Grundsätzlich kann unter Linux sowohl smb (Samba) oder rsync verwendet werden, die entsprechenden Daemons werden allerdings vorausgesetzt. Ein Linux-User kann nun wählen ob er partiell ein Backup erstellen will (also nur eines Teils seiner Daten) oder ein Full-Backup des ganzen System von „/“ an abwärts.

Die erste Variante sieht einen Share „/backup“ vor, auf dem der User „backupp“ Zugriff haben muss. Alles darin wird gesichert. Bei der Full-Backup Variante muss der User „backupp“ Zugriff auf alle zu sichernden Files haben, am besten Lese- und Schreibzugriff, da nur so auch Restores ausgeführt werden können.

Leider ist der User „backupp“ kein Domänen-Bentutzer, da deren Einbindung unter Linux relativ schwierig ist, da jeder Host seinen eigenen Daemon betreibt. Das Passwort für den entsprechenden lokalen User, muss jeweils im Config-File eingetragen werden.

9.3.11.2 Windows-Varianten

Unter Windows gibt es auch zwei Wege um Backups mit BackupPC zu erstellen. Will man zur Übertragung rsync benutzen, ist eine Cygwin-Installation mit einem rsync-Daemon Voraussetzung.

Der Standard-User wird aber den Weg über die Windows-Freigaben wählen. Auch dort kann man sich einen Share „backup“ erstellen, der dann gesichert wird oder Alternativ werden die Standard-Shares der Laufwerke verwendet („C\$“, „D\$“). Voraussetzung dafür ist, dass der Domänen-User backup_pc als lokaler Admin eingetragen ist.

9.4 Lokale Backup Lösung

9.4.1 Imaging

Mit einem Image wird das komplette System in eine Datei gesichert. Dies geschieht aus Geschwindigkeitsgründen über das Filesystem, kann aber auch Raw (also Bit-für-Bit) erfolgen. Acronis TrueImage unterstützt beide Modi.

9.4.1.1 BootCD vs. lokale Installation

TrueImage kann unter Windows installiert werden und von dort aus verwaltet werden. Es bietet an Task zu erstellen die regelmässig das System sichern. Ebenfalls bietet es die Option Backups im laufenden Betrieb zu erstellen.

Die BootCD ist betriebssystemunabhängig, basiert allerdings auf Windows (BartPE). Damit lassen sich mit einer fast identischen Oberfläche jegliche Partitionen/ Festplatten sichern.

9.4.1.2 Zentrales Management

Auf einem zentralen Windows-Server kann die Management Konsole installiert werden. Sie erfasst alle TrueImage Installationen im Netz und stellt dazu Funktionen bereits, so lässt sich ein Backup und ein Restore vom Server aus steuern wie auch

ein geplanter Task einrichten.

Für unsere IT-Abteilung könnte dies von Vorteil sein, da sie einem User direkt helfen kann Backups zu erstellen und dafür nicht vor Ort sein muss.

9.4.1.3 Restore einzelner Files

Ein Image lässt sich mit Acronis laden und durchsuchen. Einzelne Files davon können direkt wiederhergestellt werden.

Dies ist nur bei den Unterstützten Dateisystemen möglich, Raw-Image lassen sich nur komplett wiederherstellen.

9.4.2 Datenbackup

Ist es nicht unbedingt nötig das ganze System zu sichern, kann auch ein Datenbackup gemacht werden. Dies ist die empfohlene Variante für regelmässige Backups. In grösseren Abständen kann auch noch ein Image erstellt werden, so dass nicht alle Software neu installiert werden muss, sollte es zum Ernstfall kommen.

9.4.2.1 Linux (rsync)

Linux bietet mit rsync ein Tool, das auf einfachste Weise Backups auf andere Partitionen oder gar auf entfernte Systeme legen kann. Am schönsten ist eine Full/Incremental-Strategie, die jeweils wöchentlich per cron ein Fullbackup einer gegebenen Quelle macht und unter der Woche täglich ein Incremental. Nach 6 Incrementals (am 7. Tag kommt ja wieder ein Full) sollen die Incrementals gelöscht werden und ab dem 8. Tag wieder neue Incrementals gemacht werden.

Dank Sym- und Hardlinks bietet Linux die Möglichkeit jedes Incremental Image wie ein Full-Image aussehen zu lassen, indem es einfach auf die nicht veränderten Daten zeigt. Somit lässt sich direkt von einem Incremental ein Restore machen ohne den mühsamen Weg über unzählige Stationen.

Scripts und Beispiele finden sich in der Anleitung im Anhang.

9.4.2.2 Windows (NTBKP)

Mit NTBKP lässt sich sogar ein Komplettsystem sichern, dazu muss der System State mitgeschert werden. Sollte man nun ein Restore des ganzen Systems benötigen, kann man ein Image aufspielen und mit Hilfe vom NTBKP und dem System State den altern Status wiederherstellen.

Wegen Platzgründen sollte dies allerdings nicht allzu häufig gemacht werden. Um nicht ständig selbst ans Backup denken zu müssen, empfiehlt es sich einen Task einzurichten, der dies regelmässig auf ein vordefiniertes Medium macht.

Sollten nur die wichtigsten Daten gespeichert werden, kann dies auch auf dem User-Home geschehen, das zusätzlich auf dem Server gesichert wird.

9.5 Security

Immer wenn eine neue Lösung eingeführt werden soll muss man sich auch Gedanken machen über deren Sicherheit. Intern gibt es einige Standards die einzuhalten sind und andere sind „Best Practise“, also Erfahrungswerte oder weit verbreitete Ansichten wann etwas als sicher angeschaut wird.

9.5.1 Berechtigungen

Grundsätzlich sollte alles verboten sein, das ist klar. Nur gibt es hier Einschränkungen der Machbarkeit. Mit Berechtigungen vorsichtig umzugehen ist grundsätzlich richtig, am richtigen Ort müssen sie aber auch vorhanden sein.

Um unter Windows ein Backup zu machen muss man einen User aus dem Active Directory bei sich Berechtigungen geben. Will man auf einen Standard-Share wie „C\$“ zugreifen muss man lokale Administratorenrechte haben.

Möchte man dies etwas feiner einstellen, sollte man die Variante mit dem backup-Share wählen und dem User nur Rechte auf diesem Share geben (am besten nur diesem User, da sonst der Schutz von sensiblen Daten gefährdet ist).

Unter Linux sollte auch entweder die Rechte auf den zu sichernden Share gelegt werden oder sonst ein zusätzlicher Schutz bei der Konfiguration der „authorized keys“ verwendet werden (Siehe 8.2.1.3 SSH und Key-Exchange).

Vor den Eintrag des Keys kann folgendes geschrieben werden:

```
-----  
from="ipabkpsrv.trivadis.com"  
-----
```

Somit werden nur Verbindungen von diesem Host aus möglich sein.

9.5.2 Login

Die Überprüfung des Logins übernimmt das LDAP (gemäss Apache-Konfiguration, siehe 8.2.1.1 Apache2 mit mod_perl und mod_auth_ldap).

Unabhängig davon ob der Apache-Daemon unter SSL (https) läuft, sollte zumindest die Überprüfung der Credentials über eine gesicherte Verbindung erfolgen.

Voraussetzung dafür sind mod_ssl und ein Zertifikat.

Leider ist mir das bei meinem Server nicht gelungen, er läuft als Workaround ohne SSL, was wunderbar funktioniert. Gemäss Trivadis-Richtlinien, muss er aber spätestens im produktiven Stadium „LDAP over SSL“ unterstützen.

9.5.3 Dienste

Da auf einem Server so wenig Dienste wie möglich laufen sollten, habe icha auch dies geprüft mittels nmap (Portscanner):

```
-----  
ipabkpsrv 0 # nmap -v -sS ipabkpsrv  
-----  
Starting Nmap 4.01 ( http://www.insecure.org/nmap/ ) at 2006-03-30 16:55  
CEST  
DNS resolution of 1 IPs took 0.00s. Mode: Async [#: 2, OK: 1, NX: 0, DR:  
0, SF: 0, TR: 1, CN: 0]
```

IPA: Client Backup Services

```
| Initiating SYN Stealth Scan against IPABKPSRV.trivadis.com |
| (172.16.34.250) [1672 ports] at 16:55 |
| Discovered open port 443/tcp on 172.16.34.250 |
| Discovered open port 22/tcp on 172.16.34.250 |
| Discovered open port 80/tcp on 172.16.34.250 |
| The SYN Stealth Scan took 0.16s to scan 1672 total ports. |
| Host IPABKPSRV.trivadis.com (172.16.34.250) appears to be up ... good. |
| Interesting ports on IPABKPSRV.trivadis.com (172.16.34.250): |
| (The 1669 ports scanned but not shown below are in state: closed) |
| PORT      STATE SERVICE |
| 22/tcp    open  ssh |
| 80/tcp    open  http |
| 443/tcp   open  https |
|
| Nmap finished: 1 IP address (1 host up) scanned in 0.195 seconds |
|                               Raw packets sent: 1672 (73.6KB) | Rcvd: 3347 (141KB) |
```

Die hier aufgeführten Ports sind SSH (22), Apache (80) und Apache über SSL (443). Der https-Port diente nur zu Testzwecken, auf einer produktiven Maschine würde dann Apache nur noch auf einem Port laufen, je nach dem ob SSL verwendet wird oder nicht.

10 Testen

10.1 Testfälle

Die aufgeführten Punkte sind die Bedingungen die erfüllt sein müssen für einen erfolgreichen Test.

10.1.1 Zentrales Backup

10.1.1.1 1.0: Webserver erreichbar (ipabkpsrv.trivadis.com/cgi-bin/BackupPC_Admin)

- Gestartet sein
- Auf Port 80 laufen
- CGI korrekt installiert sein

10.1.1.2 1.1: Login erforderlich für ipabkpsrv.trivadis.com/cgi-bin/BackupPC_Admin

- Konfiguration des LDAPs mit mod_auth_ldap



10.1.1.3 1.2: Login mit AD/LDAP Credentials möglich

- Korrekte Anbindung ans LDAP
- Austausch von LDAP/AD

10.1.1.4 2.0: Anzeige der Seite gemäss Rollenverteilung

- Normaler User:
 - Auswahl der eingetragenen Clients in DropDown Liste
 - Log-Files der eigenen Clients anschauen
 - Client Konfigurationsfile anschauen
 - Keine Administrationswerkzeuge
- CGI-Admin User
 - Keine Clients
 - Server Logfiles anschauen
 - Konfiguration neu laden
 - Anschauen der Server Konfiguration

10.1.1.5 2.1 Korrekte Darstellung der Seite

- CSS wird geladen
- Bilder werden geladen

10.1.1.6 2.2 Alle Browser bieten das gleiche (funktional und visuell)

- Standardkonformes HTML und CSS

10.1.1.7 2.3 Links im Config-File führen zur richtigen Stelle in der lokalen Dokumentation

- Installation der lokalen Dokumentation
- Korrektes Setzen der Pfade in der Serverkonfiguration

10.1.1.8 3.0 Backup-Jobs anschauen

10.1.1.9 3.1 Backup-Jobs starten

- Programme vorhanden
- Execute-Recht gesetzt
- User hat genügend Rechte

10.1.1.10 3.2 Backup-Jobs stoppen

- User hat genügend Rechte

10.1.1.11 4.0 Backups browsen

- Richtige Ordner-Struktur
- Genügend Rechte in den Verzeichnissen

10.1.1.12 4.1 Restore starten

- Programme vorhanden
- Execute-Recht gesetzt
- Write-Berechtigung auf Client
- Berechtigung für Programm

10.1.1.13 4.2 Files als ZIP direkt downloaden

- Zugriff auf Files
- ZIP Funktion aktiviert

10.1.1.14 5.0 Backups enthalten alle gewünschten Dateien

- Zugriff auf Dateien gewährleistet

10.1.1.15 5.1 Abgebrochene Backups kreieren ein „Partial Backup“

- Crash nur auf Client-Seite so dass BackupPC ein Partial anlegen kann

10.1.1.16 5.2 Restore von Daten führt zum gewünschten Ergebnis

- Rechte sind vorhanden

10.1.2 Lokales Backup

10.1.2.1 1.0 Installation der Software

- Berechtigung für Download
- Recht zum installieren von Software

10.1.2.2 2.0 Backup konfigurieren

- Genügende User-Anleitung

10.1.2.3 3.0 Backup ausführen

- Genügend freier Speicherplatz

10.1.2.4 3.1 Image auf USB Disk

- Genügend freier Speicherplatz

10.1.2.5 3.2 Zwei Versionen speichern

- Genügend freier Speicherplatz

10.1.2.6 4.0 Restore möglich

- Vollständiges Image

10.1.2.7 4.1 Restore einzelner Files möglich

- Dateisystem-Image
- Vollständiges Image

10.1.2.8 5.0 Automatisches Backups einrichten

- Truelmage muss im Hintergrund laufen

10.1.2.9 6.0 Funktionalität via BootCD

- Korrektes Brennen der CD
- Festplatten lesbar

10.1.2.10 6.1 Zugriff auf Festplatten funktioniert

- Genügend Rechte
- Standard-Treiber reichen für Lesezugriff

10.2 Ergebnisse

10.2.1 Zentrales Backup

| Testfall | Bezeichnung / Anweisungen | Soll-Ergebnis | Ist-Ergebnis | ok | ko | To Do |
|----------|---|--|--|-------------------------------------|--------------------------|------------------------------|
| 1.0 | Webserver erreichbar (ipabkpsrv.trivadis.com/cgi-bin/ BackupPC_Admin) | Webserver gibt antwort | Webserver gibt antwort | <input checked="" type="checkbox"/> | <input type="checkbox"/> | - |
| 1.1 | Login erforderlich für ipabkpsrv.trivadis.com/cgi-bin/ BackupPC_Admin | Webserver reagiert mit Passwortfrage | Passwortfrage erscheint mit korrektem Text | <input checked="" type="checkbox"/> | <input type="checkbox"/> | - |
| 1.2 | Login mit AD/LDAP Credentials möglich | Anfrage ans LDAP soll Benutzer authentifizieren („LDAP over SSL“) | Anmeldung über Domänen-User/PW möglich | <input checked="" type="checkbox"/> | <input type="checkbox"/> | LDAP over SSL |
| 2.0 | Anzeige der Seite gemäss Rollenverteilung | Als normaler Benutzer sollte man seine Hosts sehen, als Admin nur die Admin-Funktionen (keine Daten) | User „sto“ sieht ltsto und ltsto- linux (seine Clients), „backup_pc“ als Admin sieht nur die Admin- Funktionen | <input checked="" type="checkbox"/> | <input type="checkbox"/> | - |
| 2.1 | Korrekte Darstellung der Seite | Bilder und CSS sollten geladen werden | Bilder und CSS wird korrekt geladen | <input checked="" type="checkbox"/> | <input type="checkbox"/> | - |
| 2.2 | Alle Browser bieten das gleiche (funktional und visuell) | Egal welcher Browser, es sollte immer gleich aussehen und das selbe bieten | Getestet mit IE 6.0, Firefox 1.5.1, Opera 9, Konqueror JavaScript macht etwas Probleme, dies ist aber nur Luxus, Funktionalität ist die gleiche. | <input checked="" type="checkbox"/> | <input type="checkbox"/> | Java Script aktivieren |
| 2.3 | Links im Config-File führen zur richtigen Stelle in der lokalen | Jeweils richtige Sektion in der Dokumentation sollte angezeigt werden | Links werden korrekt gesetzt | <input checked="" type="checkbox"/> | <input type="checkbox"/> | - |

| | | | | | | |
|-----|--|--|--|-------------------------------------|--------------------------|---|
| | Dokumentation | | | | | |
| 3.0 | Backup-Jobs anschauen | In einer Übersicht sollte alle Jobs ersichtlich sein, inkl. Datum, Platz usw. | Übersicht funktioniert und liefert alle gewünschten Daten | <input checked="" type="checkbox"/> | <input type="checkbox"/> | - |
| 3.1 | Backup-Jobs starten | Jobs starten richtig und bestätigen dies dem User auch | Jobs lassen sich problemlos starten. Rückmeldung „backup processing“ | <input checked="" type="checkbox"/> | <input type="checkbox"/> | - |
| 3.2 | Backup-Jobs stoppen | Jobs sollte sich stoppen lassen | Stop funktioniert, das Backup hört sofort auf. | <input checked="" type="checkbox"/> | <input type="checkbox"/> | - |
| 4.0 | Backups browsen | Die verschiedenen Versionen sollte sich durchsuchen lassen | Das durchsuchen der Backups ist kinderleicht und intuitiv. | <input checked="" type="checkbox"/> | <input type="checkbox"/> | - |
| 4.1 | Restore starten | Restore wird sofort ausgeführt und Daten werden wiederhergestellt | Der Restore stellt alle gewünschten Daten wieder her, Status im Interface ersichtlich. | <input checked="" type="checkbox"/> | <input type="checkbox"/> | - |
| 4.2 | Files als ZIP direkt downloaden | Ausgewählte Files werden zu einem ZIP zusammengestellt und können dann heruntergeladen werden. | Download funktioniert prima, Files sind wie gewünscht gepackt (inkl. Ordnerstruktur) | <input checked="" type="checkbox"/> | <input type="checkbox"/> | - |
| 5.0 | Backups enthalten alle gewünschten Dateien | Backups müssen vollständig sein gemäss dem spezifizierten Share | Alle Daten werden gespeichert (sofern sie nicht geöffnet sind während dem Sichern) | <input checked="" type="checkbox"/> | <input type="checkbox"/> | - |
| 5.1 | Abgebrochene Backups kreieren ein „Partial Backup“ | Stoppt man ein Backup, sollte alle bisher gesicherten Daten in einem Partial Backup gespeichert werden | Sofort nach dem Abbruch ist das Partial Backup verfügbar und lässt sich durchsuchen, restoren usw. | <input checked="" type="checkbox"/> | <input type="checkbox"/> | - |
| 5.2 | Restore von Daten führt zum gewünschten Ergebnis | Daten werden an ihren Originalplatz wiederhergestellt. | Daten werden am erwarteten Ort wiederhergestellt | <input checked="" type="checkbox"/> | <input type="checkbox"/> | - |

10.2.2 Lokales Backup

| Testfall | Bezeichnung / Anweisungen | Soll-Ergebnis | Ist-Ergebnis | ok | ko | To Do |
|----------|---------------------------|---------------|--------------|----|----|-------|
|----------|---------------------------|---------------|--------------|----|----|-------|

| | | | | | | |
|-----|----------------------------------|--|---|-------------------------------------|--------------------------|---|
| 1.0 | Installation der Software | Software lässt sich downloaden und installieren | Downlaod Funktioniert, Installation auch. | <input checked="" type="checkbox"/> | <input type="checkbox"/> | - |
| 2.0 | Backup konfigurieren | Einrichten ist intuitiv, Festplatte lässt sich auswählen, Tool verhält sich erwartungsgemäss | Die Konfiguration ist problemlos und dem Benutzer bekannt. | <input checked="" type="checkbox"/> | <input type="checkbox"/> | - |
| 3.0 | Backup ausführen | Ziel File lässt sich auswählen, Task ist ersichtlich und läuft | Auswahl des Images ist kein Problem, Task sieht man in der Liste der Tasks und das Backup läuft | <input checked="" type="checkbox"/> | <input type="checkbox"/> | - |
| 3.1 | Image auf USB Disk | Die USB-Disk ist formatiert und bereit für die Images | USB Disk nimmt Image auf und ist mit USB 2.0 sehr schnell | <input checked="" type="checkbox"/> | <input type="checkbox"/> | - |
| 3.2 | Zwei Versionen speichern | Die USB Disk sollte 2 verschiedene Versionen des Images speichern können | Dank NTFS sind grosse Files kein Problem. Auch lassen sich mit genügend Speicherplatz zwei Versionen speichern, je nach Datenbestand auch mehr | <input checked="" type="checkbox"/> | <input type="checkbox"/> | - |
| 4.0 | Restore möglich | Beim Restore sollte ein Image angegeben werden können, welches dann wiederhergestellt wird. | Restore wird ordnungsgemäss ausgeführt und Files sind im dann wieder im alten Zustand | <input checked="" type="checkbox"/> | <input type="checkbox"/> | - |
| 4.1 | Restore einzelner Files möglich | TrueImage sollte aus einem Image einzelne Files extrahieren können | Sofern es sich nicht um eine Bit-für-Bit Kopie handelt kann TrueImage ein Image öffnen und daraus kann der User beliebig Files extrahieren. | <input checked="" type="checkbox"/> | <input type="checkbox"/> | - |
| 5.0 | Automatisches Backups einrichten | Automatische Task lassen sich einfach anlegen und sie laufen zur gewünschten Zeit. | Mit TrueImage kann man Tasks planen und diese dann ausführen lassen. Sie laufen zum angegebenen Zeitpunkt (Beim Ausschalten, beim Abmelden usw.). | <input checked="" type="checkbox"/> | <input type="checkbox"/> | - |

| | | | | | | |
|-----|--------------------------------------|---|--|-------------------------------------|--------------------------|---|
| 6.0 | Funktionalität via BootCD | CD lässt sich booten und bieten gleichwertige Funktionen zur installierten Version. | Ist das BIOS richtig eingestellt bootet der Computer von der CD und bietet dann eine fast identische Version (ohne geplante Tasks) | <input checked="" type="checkbox"/> | <input type="checkbox"/> | - |
| 6.1 | Zugriff auf Festplatten funktioniert | Die CD-Version kann auf die Festplatten lesend und schreibend zugreifen. | Auch die CD hat kein Problem mit den Festplatten. Für den schreibenden Zugriff ist ein unterstütztes Dateisystem erforderlich. | <input checked="" type="checkbox"/> | <input type="checkbox"/> | - |

11 Literaturverzeichnis

[Internet, Stand: 31.3.2006] Gentoo Installation Guide: <http://www.gentoo.org/doc/en/handbook/2006.0/handbook-x86.xml>

[Internet, Stand 31.3.2006] BackupPC Documentation: <http://backuppc.sourceforge.net/faq/BackupPC.html>

12 Glossar

13 Anhang

- Anleitung für Benutzer