Autor: Matthieu von synology-forum.de

Synology DiskStation – Inoffizielles Handbuch

NAS, Netzwerke, Apps, Clouds und mehr

DSM 4.2 - 24.03.2013

Synology DiskStation – Inoffizielles Handbuch

Inhaltsverzeichnis

Inhalt

Vor dem Lesen

Gastautoren

Ich freue mich immer, wenn andere Nutzer mir helfen, indem sie mir Texte zur Verfügung stellen, welche sie verfasst haben:

- ag_bg (iTunes-Server)

Wer über gute Kenntnisse zu den hier besprochenen Themen verfügt und ein wenig Zeit übrig hat sowie gerne schreibt, kann sich bei uns im Synology-Forum[1] melden.

Weitere Literatur

- http://synology-wiki.de
- http://synology-forum.de
- http://de.selfhtml.org
- http://de.wikipedia.org
- http://www.synology.com
- http://forum.synology.com/
- http://forum.synology.com/wiki/
- Synology Benutzerhandbuch
- *Krzysztof Janowicz*: Sicherheit im Internet. 3. Auflage, O'Reilly Verlag, Köln, 2007, ISBN: 978-3-89721-715-7
- *Jon Masters, Richard Blum*: Professional Linux Programming. Wiley Publishing, Indianapolis, 2007, Reprint by Wiley India, ISBN: 10-81-265-1204-0
- *Steffen Wendzel, Johannes Plötner*: Einstieg in Linux. 3., aktualisierte Auflage 2008, 1. Korrigierter Nachdruck 2009, Galileo Press, Bonn, 2008, ISBN: 978-3-8362-1089-8
- http://itari.syno-ds.de

Danksagung

Ich möchte mich bei den Nutzern des deutschen Synology Forums (http://synology-forum.de) für ihre Mithilfe und Fehlerkorrektur sowie ihre Ideen bedanken.

Außerdem möchte ich hier explizit die Nutzer erwähnen, welche immer wieder neue Texte gelesen und – fachlich wie sprachlich – vielerlei Fehler fanden:

- MJFox/Kamil
- Manuel_bo
- coolhot
- Hannibal7777

Lizenz

[1] http://www.synology-forum.de, oder direkt an den Autor: matthieu-ds@hotmail.de

Sie dürfen:
das Werk bzw. den **Inhalt vervielfältigen, verbreiten und öffentlich zugänglich machen**
Zu den folgenden Bedingungen:
Namensnennung — Sie müssen den Namen des Autors/Rechteinhabers in der von ihm festgelegten Weise nennen.
Keine kommerzielle Nutzung — Dieses Werk bzw. dieser Inhalt darf nicht für kommerzielle Zwecke verwendet werden.
Keine Bearbeitung — Dieses Werk bzw. dieser Inhalt darf nicht bearbeitet, abgewandelt oder in anderer Weise verändert werden.

(Dies ist nur eine Zusammenfassung und nicht rechtlich gültig![2])

Ich bin einer Nutzung in einem anderen Rahmen stets aufgeschlossen. Bei Interesse findet man mich im deutschen Forum oder per Mail.

Haftung

Dieses Dokument ist keine Publikation einer offiziellen Stelle. Das Dokument erhebt weder den Anspruch auf Vollständigkeit noch auf Fehlerfreiheit. Für Fehler in diesem Dokument übernimmt der Autor keinerlei Haftung. Die Verwendung der beschriebenen Vorgehensweisen erfolgt ausdrücklich auf eigene Gefahr.

Hinweise zur Verwendung

- Dieser Guide wurde zur Firmware „DSM 4.2-3202“ geschrieben. Sollten Sie eine andere Firmware verwenden kann es gewisse Unterschiede geben. Aus diesem Grund kann ich außerdem nicht garantieren, dass alle Screenshots aktuell sind bzw. auf allen Geräten der Firma Synology identisch aussehen. Im Zweifelsfall konsultieren Sie bitte das Handbuch oder die integrierte DSM-Hilfe.
- Sämtliche Links welche sich auf die DiskStation beziehen (z.B. http://DiskStation:5000/) funktionieren in Ihrem Netzwerk wahrscheinlich nicht. Die Bezeichnung „DiskStation“ müssen Sie daher entweder durch die IP oder den Namen ihrer DiskStation ersetzen. Wenn Sie im LAN arbeiten empfiehlt es sich nicht, die DDNS-Adresse zu verwenden, da einige Router dies nicht korrekt umsetzen können.

Bisher erschienen

Die folgenden Versionen wurden bisher von mir veröffentlicht:

- Synology DiskStations – Inoffizielles Handbuch (vom 31.8.2011)
- Synology DiskStations – Inoffizielles Handbuch (vom 04.01.2011)
- Synology DiskStations – Inoffizielles Handbuch (vom 07.08.2010)
- Synology DiskStations - Kleiner Guide (vom 23.09.2009)
- Synology DiskStations - Kleiner Guide (vom 09.08.2009)
- Synology DiskStations - Kleiner Guide (vom 01.06.2009)
- Synology DiskStations - Kleiner Guide (vom 12.04.2009)
- Synology DiskStations - Kleiner Guide (vom 13.03.2009)
- Synology DiskStations - Kleiner Guide (vom 25.02.2009)
- Synology DiskStations - Small Guide (from the 29.04.2009)

[2] Quelle: Commons Deed von http://creativecommons.org/licenses/by-nc-nd/3.0/de/

Warenzeichen & Copyright

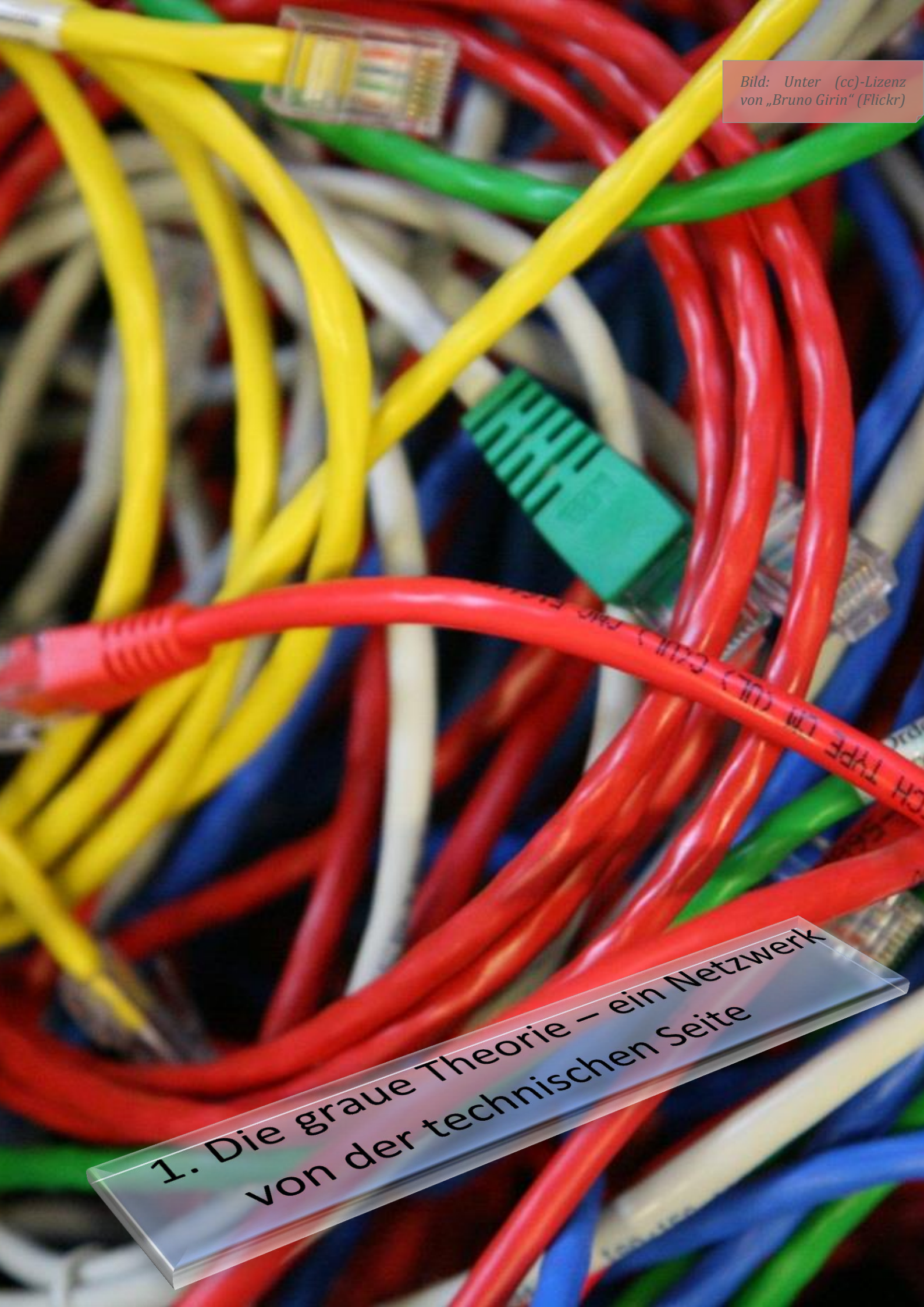


Bild: Unter (cc)-Lizenz von „Bruno Girin“ (Flickr)

1. Die graue Theorie – ein Netzwerk von der technischen Seite

1 Die graue Theorie – ein Netzwerk von der technischen Seite

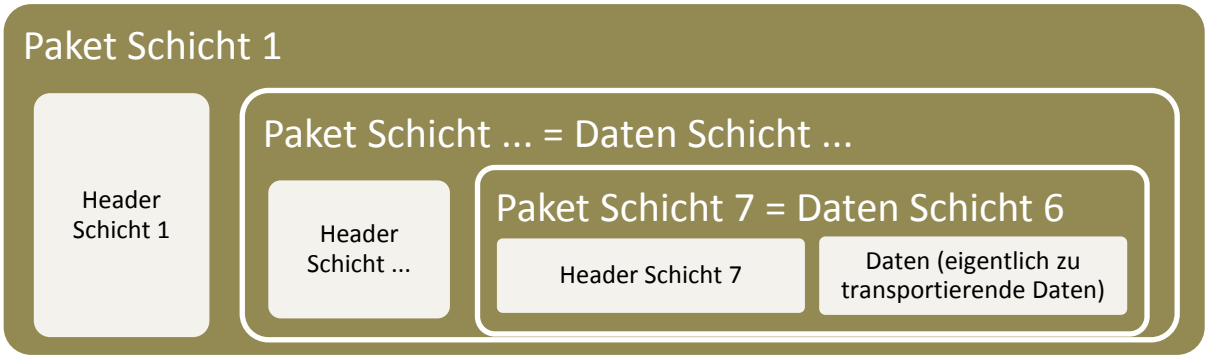
Die Handhabung eines NAS mag dank grafischer Oberfläche denkbar einfach sein, doch im Hintergrund arbeiten noch dieselben Mechanismen wie bei den großen Servern. Viele der Technologien und Zusammenhänge werden deutlich einfacher wenn man weiß, wie die Anwendung arbeitet und mit welchem Ziel sie entwickelt wurden. Wer das Kapitel überspringen möchte, dem empfehle ich später zurückzukehren und bei Bedarf einzelne Punkte nachzulesen.

Das bekannteste Modell stammt von der „International Standardisation Organisation“ und nennt sich „Open Systems Interconnect“ oder schlicht OSI-Modell. Es entstammt eigentlich schon älteren Überlegungen zu Netzwerken, kann jedoch nahezu nahtlos auf die aktuelle Technik angewendet werden.

Das OSI-Modell besteht aus 7 Schichten. Jede mit eigenen Aufgaben. Doch wie diese gelöst werden, ist dem jeweiligen Protokoll bzw. der Anwendung überlassen. Besonders wichtig innerhalb dieses Prozesses ist auch die „Encapsulation“[3]. Dadurch wird beschrieben, dass jede Schicht zu den ihr übergebenen Daten einen „Header“ hinzufügt. Dieser enthält wichtige Informationen wie Adressen für diese Schicht, wird von den darunterliegenden Schichten jedoch unverändert als Daten behandelt. Damit kommen zu den eigentlichen „Nutzdaten“ häufig auch eine große Menge an Informationen die für die Übertragung notwendig sind, am Ziel jedoch wieder entfernt werden.

Darüber hinaus können Schichten auch ihnen übergebene Daten in kleinere Einheiten unterteilen. Sie müssen dann jedoch am Ziel wieder korrekt zusammengesetzt werden.

„Encapsulation“



1.1 Was nicht im OSI ist: Die PC-Hardware

Eigentlich greift da wo ich anfangen möchte das OSI-Modell noch nicht, denn es beschäftigt sich nur mit der am Netzwerk beteiligten Hardware. Doch erst einmal müssen die Daten natürlich von einer Festplatte geladen werden und genau da werde ich auch beginnen.

Der eigentlich „erste Schicht“ definiert, wie das einzelne Bit übertragen wird. Also welche Funkwelle für 0 oder 1 steht, ähnliches bei Kabeln. Das meist verwendete Ethernet-Verfahren beschreibt Schicht 1 und 2, weshalb ich mich erst später damit beschäftigen werde, sobald Schicht 2 theoretisch abgehandelt wurde.

[3] Englisch für “Kapselung”

1.1.1 Raids

Bevor die DiskStation in Betrieb genommen werden kann, ist ein Thema von großer Bedeutung: Was passiert, wenn die Festplatte in die Knie geht? Steht die gesamte Firma dann für mehrere Stunden oder Tage still? Da solche Ausfälle häufig unbezahlbar sind, gibt es natürlich ein Gegenmittel. Sogenannte Raids kopieren alle Dateien auf verschiedene Festplatten, um im Falle eines Defektes ohne Datenverlust weiterarbeiten zu können. Bei den größeren DiskStations, welche Hot-Swap-fähig sind, können Sie sogar im laufenden Betrieb die defekte Platte austauschen. Komplette Sicherheit kann allerdings nicht gewährleistet werden, denn wenn man eine Datei löscht, fehlt sie danach nicht nur auf einer Platte, sondern auf allen. Doch mit Backups, welche in diesem Fall helfen können, werden wir uns noch früh genug auseinandersetzen. Da es nicht immer möglich und mit einem großen Risiko verbunden ist, die Raids im Nachhinein zu ändern, sollte man von Anfang an die Konfiguration wählen, welche für einen den meisten Sinn ergibt.

Hier ein kurzer Überblick, über die von den DiskStations unterstützten Möglichkeiten:

Raid-Level	Benötigte Festplatten	Tolerierte, gleichzeitige Ausfälle	Kapazität des neuen, logischen Laufwerks (Laufwerke/Größe)
Kein Raid	1	0	1/1
Raid-0	2,3,4,5	0	5/5
Raid-1	2	1	2/1
Raid-5	3,4,5	1	5/4
Raid-6	3,4,5	2	5/3
SHR	Min. 2	wählbar	Siehe Text

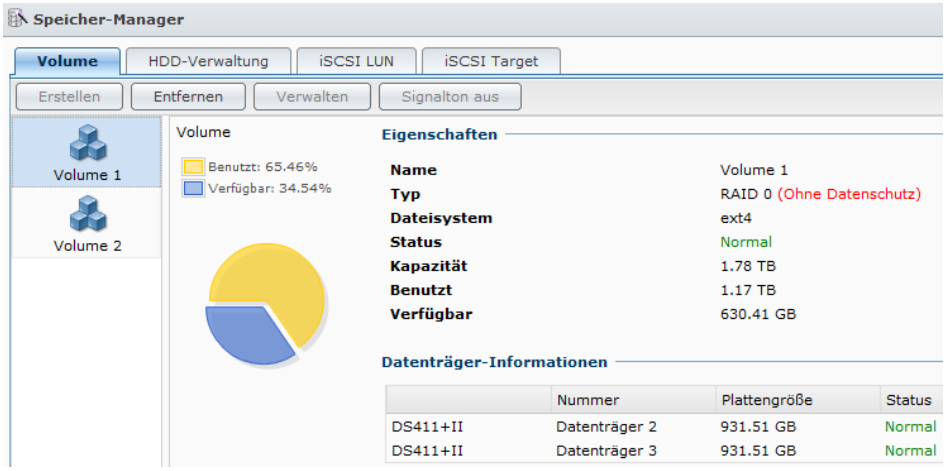
Kleine Erklärung: „Benötigte Festplatten“ gibt an, wie viele Festplatten verwendet werden können. „Tolerierte, gleichzeitige Ausfälle“ gibt an, wie viele Festplatten Schaden nehmen dürfen, ohne dass man Angst vor Datenverlust haben muss. „Kapazität“ gibt an, wie groß das neue, virtuelle Laufwerk wird (z.B. 5/3: Wenn man fünf Festplatten einsetzt, hat das neue Laufwerk die Größe von drei Laufwerken).

Beachten sollte man, dass die Platte mit der geringsten Kapazität immer die Kapazität aller anderen vorgibt. (z.B.: Man hat 4 Festplatten zu je 3 TB und eine mit 1 TB, dann ist die Kapazität am Ende so groß, als wäre 5x1 TB verbaut.) Es empfiehlt sich also, stets dieselben Festplattengrößen zu verwenden. Wer ganz sicher sein möchte, greift zu Festplatten verschiedener Hersteller. Sollte es dann zu Serien-bedingten Problemen kommen, kann man schnell ausweichen.

Eine Ausnahme ist nun das Synology Hybrid Raid, oder SHR. Es ermöglicht die Nutzung von verschiedenen Festplattengrößen bei wählbarer Redundanz. Doch dazu gleich noch mehr.

Doch eines sollte man trotz Raid nie vergessen: **Einen Ersatz für Backups gibt es nicht!**

Mehr Informationen zu diesem Thema enthält Kapitel 4, „Backup**“.** In Erfahrungsberichten hat sich gezeigt, dass ein Raid-0 zur Datenrettung sehr ungeeignet ist. Es kopiert Teile auf eine, Teile auf eine andere Platte, wodurch das Zusammensetzen sich sehr schwierig bis gänzlich unmöglich gestalten kann. Selbiges gilt auch für Raid-5 und Raid-6. Jedoch ist hier zumindest die Rettung aufgrund der Verteilung möglich.



1.1.2 SHR/LVM

Was Synology mit „Hybrid Raid" betitelt hat, ist für Linux nichts anderes als ein LVM oder Logical Volume Manager mit zusätzlichen Automatismen. Unter Linux existiert diese Technik bereits seit einigen Jahren, doch ist sie recht kompliziert zu handhaben.

Synology hat diesen LVM erweitert indem eine wählbare Anzahl von Festplatten stets ausfallen können, ohne dass Daten verloren gehen.

Der LVM an sich abstrahiert die Festplattenkontrolle. Etwas zu abstrahieren ist ein wichtiger Bestandteil des Linux-Konzepts. Obwohl viele verschiedene Systeme unter Linux laufen, so sind die benötigten Befehle doch immer die gleichen. Denn alle Befehle greifen nur auf den Betriebssystemkern zu. Dieser Kernel übersetzt dann mittels Treiber den Aufruf je nach Hardware. So ist es auch unnötig zu wissen, auf welcher Festplatte eine Datei genau liegt, denn der LVM ist mittels Treiber in den Kernel integriert. In Verbindung mit der Synology-Automatik für Raid-Wahl wird so der gesamte vorhandene Speicherplatz zusammengefasst um möglichst viel aus dem gegebenen Szenario zu holen und die Wahl der Raids einer Automatik zu überlassen.

Eingriffe in diese Technik gewährt nur die Synology-spezifische Konfigurationsoberfläche als Teil des DSM. Synology hält diesen Teil recht gering um die Administration zu vereinfachen. Über die Kommandozeile eröffnen sich jedoch vielfältige Möglichkeiten um auf den LVM Einfluss zu nehmen, denn Synology hat alle Standard-Programme integriert.

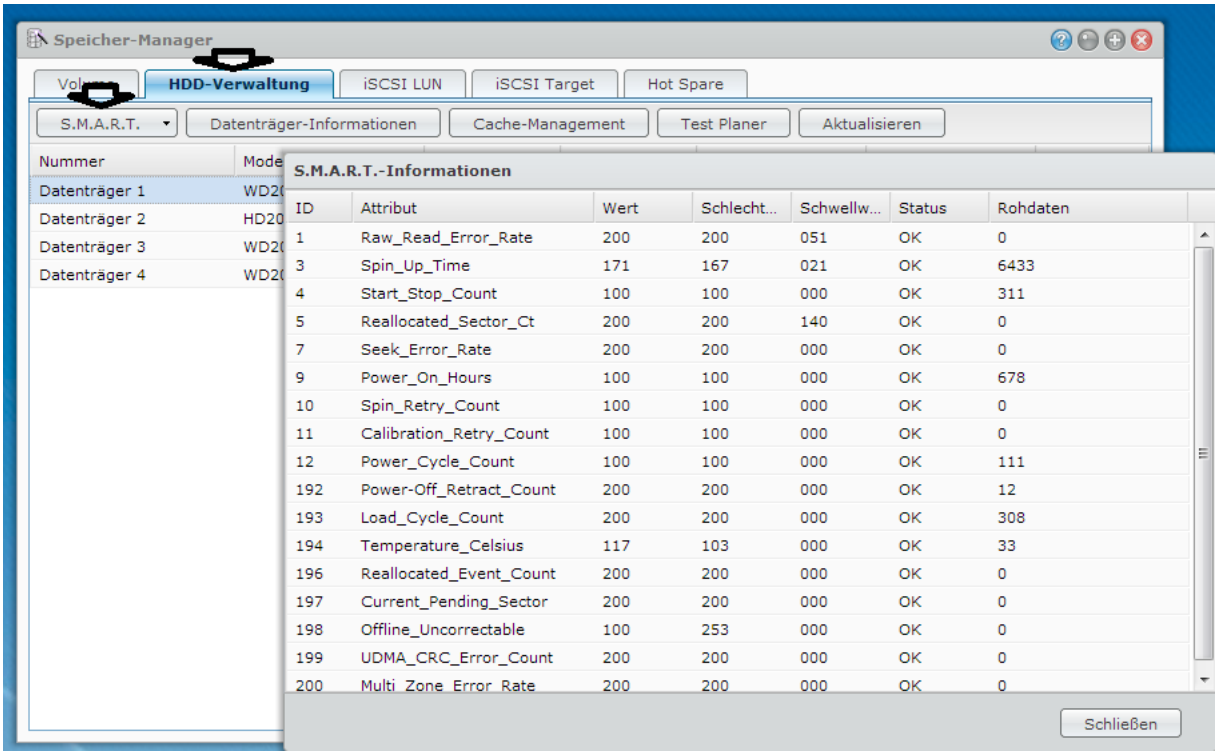
Um die genaue Kapazität von herkömmlichem Raid und SHR zu vergleichen hat Synology eine kleine Webapplikation gestaltet: http://www.synology.de/support/RAID_calculator.php?lang=deu.

1.1.3 S.M.A.R.T.

„Self Monitoring, Analysing and Reporting Technology" ist die Bezeichnung für einen Dienst, welcher wichtige Daten über Festplatten sammelt. Diese Daten enthalten ganz einfache Angaben wie die Anzahl der Betriebsstunden aber auch komplexere, wie die der defekten Sektoren. Laut einer großen Feldstudie von Google[4] sollen mehr als die Hälfte aller Festplattenausfälle anhand von SMART-Werten vorhersehbar sein. Die DS kann entsprechende Tests auf den eingebauten Festplatten durchführen und deren Ergebnisse auf Basis von Vorgaben der Hersteller interpretieren. Doch die meisten dieser Werte sind statisch, eine wirklich intelligente Problemerkennung kommt dabei nicht

[4] http://labs.google.com/papers/disk_failures.pdf

zustande. Google zufolge bringt erst eine Langzeitbetrachtung die gewünschten Erfolge. Bei der Verletzung der vom Hersteller festgelegten Grenzwerte schlägt die DS dann deutlich Alarm.



1.2 Schicht 1: Hardware (Bitübertragungsschicht)

Die IEEE („Institute of Electrical and Electronics Engineers") legt fest, wie man auf ein Medium wie Luft oder Kupferkabel eine 0 oder 1 aufbringt und wie das Medium beschaffen sein muss. Dazu gehören u.a. auch Stecker sowie die zu verwendenden Frequenzen. Bekannt sind meist die WLAN-Standards 802.11 sowie Ethernet (802.3). Es gibt jedoch auch einige weitere, etwa für Glasfaser-Verbindungen.

1.3 Schicht 2: Sicherungsschicht

Nun, da die Daten auf dem Weg in Richtung Netzwerk sind, müssen Sie nur noch an der Netzwerkschnittstelle vorbei. Aber die möchte ich jetzt nicht auch noch auseinander nehmen. Daher geht es jetzt mit dem technischen Verfahren um die Übertragung zu sichern und den Transportweg zu finden weiter. Also mit Schicht 2 des theoretischen Modells. Und wie bereits angekündigt, deckt das heute übliche Ethernet-Verfahren die beiden ersten Schichten ab.

1.3.1 Ethernet

Die recht simple Idee hinter Ethernet ist die Verbreitung von Informationen über Hochfrequenzen in einem Kabelnetzwerk. Jedes Paket wird dabei mit zwei 48-Bit-MAC-Adressen versehen (MAC hat in diesem Fall nichts mit den Macintoshs von Apple zu tun), welche einmalig sind. Diese Adressen gehören zu den Netzwerkschnittstellen von Sender und Empfänger. Jedes netzwerkfähige Gerät auf dieser Welt hat eine eigene. So zumindest die Theorie – in der Praxis bringt meist das Betriebssystem die MAC-Adresse an ein Paket an. Das hat zur Folge, dass auch ein Betriebssystem die MAC-Adresse der eigenen Schnittstelle per Software zeitweilig ändern kann. Somit ist es sehr wohl möglich Adressen zu fälschen. Glücklicherweise werden MAC-Adressen nicht weltweit genutzt, sondern nur im LAN. Geräte auf Schicht 2, etwa ein Switch, arbeiten mit MAC-Adressen um den Weg zum Ziel zu

bestimmen. Im weltweiten Verkehr benötigt man dagegen Schicht 3 und damit Router die komplexe Wege anhand von IP-Adressen bestimmen.

Sobald jetzt von Informationen in Form von Paketen geredet wird, sind Sie in Schicht 2 angelangt, denn es geht nicht mehr um die physikalische Übertragung der Daten auf einem Kabel oder einem anderen Medium und sei es Luft. Doch je größer die Netzwerke werden, desto schwieriger wird es Kollisionen zu vermeiden. Auch die Prüfung einer vollständigen und unveränderten Übertragung ist daher Pflicht, kann aber auf verschiedenen Schichten abgehandelt werden.

Alternativ zu Ethernet gibt es beispielsweise das Token-Ring-Verfahren[5] was jedoch ein ringförmiges Netzwerk (jeder Teilnehmer mit 2 Schnittstellen) ohne Unterbrechung voraussetzt. Dabei wandern die Daten stets einmal reihum, um ihre Unversehrtheit zu bestätigen. Das sorgt jedoch für mehr Kabelsalat, höhere Ausfallquoten und längere Wartezeiten für die Pakete. Für andere Medien wie Lichtwellenleiter oder Luft kommen auch andere Standards auf Schicht 2 zum Einsatz, die häufig jedoch wie WLAN noch einmal komplexer funktionieren.

Doch um noch einmal kurz auf die technische Seite zurück zu kommen: Ethernet legt auch fest, wie Kabel und Stecker gefertigt werden müssen und in welchen Frequenzen die Daten übertragen werden. Doch zu diesen Cat-Kabeln und den verschiedenen Standards gibt es mehr in Kapitel 7.1.

1.3.2 Jumboframes

Aus früheren Tagen stammt die Festlegung, dass ein Paket von Daten, welches an Ethernet auf Schicht 2 übergeben werden darf, maximal 1.518 Bytes umfasst. Diese Menge wird als „Maximum Transmission Unit“ (zu Deutsch etwa „maximale Übertragungseinheit“), oder kurz „MTU“ bezeichnet. Ethernet ist die gebräuchlichste Transportform in lokalen Netzwerken. Damals entschied man sich für eine derartige Festlegung, da Fehler in der Übertragung recht häufig vorkamen und dann das Paket erneut gesendet werden musste. Umso kleiner das Paket damals also war, umso schneller ließ es sich erneut senden. Nun hat in den letzten Jahren die Verbesserung der Netzwerktechnologie aber dazu geführt, dass Fehler viel seltener auftreten. Da die Pakete relativ klein sind und sie nun deutlich schneller eintreffen, spielt unter anderem die Rechengeschwindigkeit eine größere Rolle. So dauert es relativ lange, bis überprüft werden konnte, ob das Paket so angekommen ist wie es sollte. Dem gegenüber steht die Tatsache, dass größere Pakete auch stets eine größere Verzögerung nach sich ziehen. Ein Switch speichert Pakete kurz zwischen und schickt sie nach Erhalt weiter. Das bedeutet also, dass ein Switch länger braucht um ein einzelnes Paket zu verarbeiten. Der „Ping“ dürfte den meisten Netzwerkinteressierten bekannt sein – und genau dieser kann bei mehreren Switchen etwas darunter leiden.

Nun aber das Problem. Die bisherigen Standards berücksichtigen Jumboframes nicht. Viele Gigabit-Switches, -Router und -Karten unterstützen zwar Jumboframes, doch das ist noch lange nicht bei allen Komponenten der Fall. Normale Jumboframes sind zwischen 1500 und 9000 Bytes groß. Aber nicht sämtliche Größen werden von jedem Gerät unterstützt. Alles in allem können Jumboframes das letzte Stück Performance aus ihrem Netzwerk holen, auf der anderen Seite sind sie aber auch kein Spielzeug, da Fehleinstellungen schnell das gesamte Netzwerk lahm legen können. Gerade wer häufig Gast-Rechner mit seinem Netzwerk verbindet oder mehrere ältere PCs einsetzt, sollte vom Gebrauch der Jumboframes lieber absehen.

[5] Mehr Infos samt Simulation: http://www.nt.fh-koeln.de/vogt/mm/tokenring/tokenring.html

Übrigens: Auch in Weitverkehrsnetzen sind größere Frames nicht unbedingt besser. So sollten Sie an der „MTU“ des DSL im Router nichts ändern.

1.3.3 Wake on LAN (WoL)

Eigentlich ist diese Schicht noch recht ungeeignet für Datentransfer, da beispielsweise die IP-Adresse noch fehlt. Doch da bei einem „Magic Packet“ wie es für WoL genutzt wird keine IP-Adresse notwendig ist, kann es bereits hier operieren. Stattdessen wird ein WoL-Signal an alle Teilnehmer eines Netzwerks geschickt. Der korrekte Empfänger wird anhand der MAC-Adresse bestimmt.

Jetzt habe ich viel gesagt, wie WoL an sein Ziel kommt, aber nicht was es macht. Die Antwort ist recht simpel: Es startet einen PC aus der Ferne. Die Netzwerkkarte des PCs ist dazu mit dem Netzteil und/oder Mainboard verbunden und löst bei Erhalt eines Paketes das Hochfahren des Gerätes aus. Das hat jedoch zur Folge, dass der Stromverbrauch im ausgeschalteten Zustand leicht ansteigt. Außerdem werden damit die Hardware-Komponenten teurer, weshalb WoL nicht in allen kleinen[6] DiskStations zu finden ist.

Bedenken sollte man aber auch, dass jeder der solche „Broadcasts“ im Netz senden kann und die MAC-Adresse des Gerätes kennt, diesen Prozess auslösen kann. Dazu sind unter Windows auch nicht administrative Rechte nötig. Die MAC-Adresse ist häufig per Aufkleber auf dem Gerät einsehbar, doch gewusst wie kann man sie auch über das Netzwerk auslesen. Die Broadcasts werden aber aus dem Internet meist vom Router geblockt, weshalb die Sicherheitsfrage meist nur im lokalen Netz besteht.

1.3.4 Virtual Private Network (VPN), (PPTP, OpenVPN)

Neben WoL arbeitet auf dieser Ebene auch eine weitaus komplexere Technologie. Denn um zwei Netzwerke effizient und sicher miteinander zu verbinden, müssen Datenpakete so tief im OSI-Modell wie möglich abgegriffen und verschlüsselt werden. Diese Chance lassen sich OpenVPN und PPTP, die von Synology dafür mitgenutzten Technologien, nicht entgehen und setzen direkt über der Hardware in Schicht 2 an. Es wird somit eine „virtuelle Netzwerkschnittstelle“ eingebunden und Pakete über diese für den PC wie gewohnt verschickt. Die Programme die für PPTP und OpenVPN zuständig sind verschlüsseln die Pakete dann und schicken sie direkt zur Gegenseite. Die entpackt selbige wieder und leitet sie wie alle anderen auch in das Netzwerk.

PPTP („Point-to-Point Tunneling Protocol“) ist der kommerzielle Ansatz zu VPN. Entwickelt wurde es von mehreren Herstellern und ist daher auch in allen namhaften Betriebssystemen von Beginn an integriert. Die Sicherheit hängt jedoch stark von der Stärke des verwendeten Passworts ab, denn es wird direkt zur Verschlüsselung der Pakete eingesetzt. Auch weitere Schwachstellen konnten in PPTP bereits ausgenutzt werden.

OpenVPN hingegen ist der Community-betriebene Ansatz[7]. Dank ihm ist VPN nicht so kompliziert wie die für große Unternehmen vorgesehenen IPsec-Tunnel, trotz angenehmer Sicherheit. Doch da für beinahe jedes Betriebssystem zusätzliche Software-Komponenten notwendig sind, ist die Einrichtung nicht ganz so einfach. OpenVPN setzt zusätzlich einen Schlüssel ein welcher benötigt wird.

[6] Welche DiskStations genau Wake on LAN haben, ist in der Vergleichstabelle aufgeführt: http://www.synology.com/deu/products/compare_spec.php

[7] Mittlerweile ist OpenVPN in die Firma „OpenVPN Technologies, Inc.“ überführt, doch die Software bleibt GPL-lizensiert und somit frei zugänglich.

Um Einrichtung und Betrieb des von Synology herausgegebenen „VPN Center“ auch für Laien zu ermöglichen, gibt es eine eigene Benutzeranleitung dafür. Die deutsche Community stellt eine Übersetzung dieses ursprünglich englischen Dokuments bereit[8].

1.4 Schicht 3: Vermittlungsschicht

Nun, da die Straßen für das Postauto gebaut und der nächste Empfänger (MAC-Adresse) auf dem Paket aufgebracht ist, geht es an die Suche nach Adresse und Weg. Und genau das ist Teil von Schicht 3 und dem häufigsten Vertreter: dem „Internet Protocol“ (IP).

1.4.1 IPv4

Während man in Ethernet also eindeutige MAC-Adressen findet die im lokalen Netzwerk verwendet werden, bietet IP einfacher handhabbare, logische Adressen.

Um den Unterschied von IP und MAC noch einmal hervorzuheben: Die IP-Adresse bleibt während der gesamten Übertragung im Normalfall identisch (es sei denn man setzt NAT ein, aber das ist ein anderes Thema). Anhand einer IP kann daher recht gut Wegfindung über mehrere Teilstrecken hinweg („Hops“) betrieben werden.

Eine IP-Adresse ist 32 Bit groß und wird in vier Felder unterteilt. Daraus ergeben sich 256 mögliche Werte pro Feld. Die IP-Adressen gehen daher von 0.0.0.0 bis 255.255.255.255; einige der Adressen sind jedoch reserviert. Zu jeder IP-Adresse gehört außerdem eine Angabe, welcher Teil das Netzwerk definiert und welcher das Gerät.

Die Trennung in Netzwerkanteil und Geräteanteil einer Adresse ist notwendig, um zu unterscheiden welche Adressen ein PC direkt erreichen kann. Wenn ein PC einen anderen kontaktieren möchte und der Netzwerkanteil von Sender und Empfänger ist identisch, so kann er direkt in Kontakt treten. Andernfalls muss er über andere Netzwerke gehen und dazu erst einmal das „Gateway“ ansteuern. Etwas praktischer verdeutlicht kann man es mit einer Postsendung vergleichen: Wenn ein Brief vom Postboten eingesammelt und in das örtliche Briefzentrum gebracht wurde, gibt es zwei Möglichkeiten: Die Postleitzahl ist identisch oder nicht. Ist sie identisch, verbleibt der Brief im Briefzentrum und geht am nächsten Tag zur Zustellung heraus. Ist die Postleitzahl hingegen nicht identisch, wird der Brief an ein größeres Briefzentrum geleitet. Das größere Briefzentrum wäre dann der Gateway.

Zurück zur IP-Adresse. Um beide Anteile nun voneinander zu unterscheiden gibt es zwei Schreibweisen, die Funktion für diese Subnetzmaske ist jedoch identisch. Die erste Schreibweise bedient sich eines „/“ und zählt die Bit, welche zum Netzwerkanteil gehören. Eine Adresse 192.168.1.2/8 macht die ersten 8 Bit („192.“) zum Netzwerk. Die zweite Schreibweise gibt, binär geschrieben, die Bits an welche zum Netzwerk gehören. So ergibt „255.240.0.0“ binär „11111111.11110000.00000000.00000000“. Gewöhnlich gibt es daher Subnetzmasken wie „255.255.0.0“. Das Aufteilen von Blöcken über Zahlen wie 128 ist eher in größeren Netzwerken üblich wenn es auf jede einzelne Adresse ankommt.

1.4.2 IPv6

Die nächste Version von IP sollte alles so viel besser machen, und daher freiwillig zum Einsatz kommen. Doch so einfach wurde es in der Praxis nicht und mittlerweile ist der Umstieg nur langsam in Gang gekommen, weil die bekannten Adressen aus Version 4 zur Neige gehen. Auch das hat

[8] http://www.synology-forum.de/showthread.html?20936-Deutschsprachige-VPN-Anleitung-zu-VPN-Center

übrigens Gründe: Man ist bei der Festlegung damals sehr freizügig gewesen und hat beispielsweise dem lokalen PC mehr als 16 Millionen Adressen zur Verfügung gestellt (zu erreichen über das 127.0.0.0/8-Netz).

Ein großes Augenmerk von IPv6 ist natürlich der Adress-Pool. Eine Adresse besteht nun aus 128 Bit. Doch auch viele andere Probleme rücken nun in den Hintergrund. So muss man Adressen nicht mehr selbst vergeben – kann es in vielen Fällen über die normale Konfiguration nicht einmal. Die Adressen für einen heimischen PC mit Internetzugang bestehen zur Hälfte aus einer Adresse des Providers und zur anderen Hälfte aus einer theoretisch frei wählbaren, die in der Praxis jedoch anhand der MAC-Adresse abgeleitet wird. MAC-Adressen sind nur über Umwege änderbar und gelten daher weithin als einmalig und eindeutig. Zusätzlich zu einer solchen öffentlichen Adresse soll jeder PC aber auch eine für das lokale Netzwerk bekommen. Es ist damit sofort klar, ob ein Paket für das lokale oder das weltweite Netz gedacht ist. Dazu kommen bei Bedarf noch Unicast und Multicast, welche Broadcast ersetzen. Der Vollständigkeit halber: Multicast versendet ein Paket an alle mit Adressen im selben Netz; Unicast an den ersten der im selben Netz antwortet.

Neben den reinen Adressen hat sich noch viel mehr getan: Es können beinahe wahllos verschiedene zusätzliche Header in IPv6 eingesetzt werden. Diese vergrößern den Header nur, wenn eine Funktion wirklich benutzt wird. Dies ermöglicht u.a.: Vorgaben eines festen Weges durch das Netzwerk („Routing-Header“), konfigurierbare Maximalpaketgrößen („Fragmentation-Header“), Authentifizierung mittels IPsec („Authentication-Header“), Verschlüsselung mittels IPsec („Encapsulation Security Payload Header“, kann zusammen mit Authentifizierung ein VPN aufbauen).

Die dennoch schleppende Verteilung der Adressen an Endkunden hat man bisher überwiegend den Betreibern der großen Netze zu verdanken. Denn IPv6 erfordert auf deren Seite etwas mehr Arbeit als für den heimischen Benutzer. Und man muss natürlich das entsprechende Know-how aufweisen. In lokalen Netzen fahren moderne Betriebssysteme schon seit einiger Zeit IPv4 und v6 gleichzeitig („Dual Stack Betrieb“).

Die deutsche Bundesregierung hat für Behörden und Verwaltung 5 Quintillionen IPv6-Adressen zugesprochen bekommen (Quintillion = Zahl mit 30 Nullen).

1.4.3 DHCP & NAT

Um IP-Adressen zu vergeben ist entweder eine manuelle Konfiguration mit vielen Zahlenkolonnen notwendig, oder das automatisierte Verfahren DHCP („Dynamic Host Configuration Protocol“). Steht ein Netzwerktreiber auf „DHCP“, so kontaktiert die Netzwerkschnittstelle sofort einen entsprechenden Server und besorgt sich von ihm die im Netzwerk üblichen Informationen wie eine eigene IP-Adresse und die gültige Subnetzmaske, sowie IP-Adresse von DNS und Gateway. Ein Gateway stellt den Zugang zu anderen Netzwerken wie dem Internet her. In einem normalen Netzwerk handelt es sich dabei also um den Router.

Bis ein Client eine Adresse über DHCP bekommt, sind jedoch mehrere Schritte notwendig. Zunächst richtet der Client einen Broadcast über das gesamte Netz auf der Suche nach einem DHCP-Server. Sind mehrere davon vorhanden, wendet sich der Client dem zu, der als erstes antwortet. Dies kann jedoch unberechenbares Verhalten bei der Adressvergabe zur Folge haben, weshalb üblicherweise nur ein DHCP-Server pro Netzwerk verwendet werden sollte. Dieser Broadcast wird auch „DHCP Discover“ genannt. Es folgt das Angebot vom Server, also das „DHCP Offer“. Der Client akzeptiert die nun erhaltenen Adressdaten mit einem „DHCP Request“ und der Server bestätigt wiederum die

abgeschlossene Konfiguration mit einem „DHCP Acknowledge“. Wird der PC heruntergefahren oder die Adresse aus einem anderen Grund nicht weiter benötigt, ist es üblich ein „DHCP Release“ zu senden und dem Server so mitzuteilen, dass die Adresse neu vergeben werden kann.

NAT („Network Address Translation“) hingegen kommt im Router zum Einsatz. Wenn ein Paket ins Internet möchte, so trifft es dort auf einen anderen IP-Adress-Bereich. Und da der Router nur eine Adresse hat, muss er sich stets als „Absender“ ausgeben und die IP-Adressen entsprechend abändern, damit der PC mit dem Internet kommunizieren kann. Beides zusammen wird von der NAT-Funktion bewältigt. Über Tabellen kann der Router dann genau zuordnen welche Antwort an welchen PC muss, auch wenn 2 PCs gleichzeitig Google aufrufen. Geht es nach den Machern von IPv6, soll NAT in absehbarer Zeit übrigens wieder verschwinden, denn die neue IP-Version sieht für jeden PC eine eigene Internet-Adresse vor. Bei Datenschützern und Sicherheitsexperten stößt dies aber auf Gegenwehr.

1.4.4 Ports

Um dies ein wenig einfacher zu erklären, stellen Sie sich ihre DiskStation als Haus vor. Ihr Router, welcher den Internetzugang regelt, bringt fast immer auch eine eigene Firewall mit. Die Firewall stellen wir uns jetzt wie einen Zaun um das Haus vor (wer will kann sich auch einen brennenden Zaun vorstellen ;-)). Um verschiedene Internetdienste, wie Webserver, E-Mail-Server, Telnet, ftp, etc. alle über dieselbe Adresse erreichen zu können ohne für jeden eine neue zu belegen, wurden Ports erschaffen. Diese Nummer, welche hinter der IP mit einem Doppelpunkt abgetrennt wird, weißt auf den Dienst hin. Jeder Port soll daher durch ein Tor in unserem Zaun veranschaulicht werden. Normalerweise sind alle Ports geschlossen, sodass keine Sicherheitslücken entstehen. Wer nun allerdings einen Server betreibt, muss bestimmte Tore öffnen um den Verkehr ungehindert fließen zu lassen. Andernfalls würden die Dienste, welche hinter den Ports warten, nicht im Internet zur Verfügung stehen. Die bekanntesten Ports sind z.B. 80 für http-Server bzw. 443 für das sichere https sowie 20/21 für ftp. Wer einen Dienst nicht im Internet benötigt, sondern nur im eigenen Netzwerk, sollte den Port nicht öffnen, da ja jeder ein kleines Sicherheitsrisiko darstellt. Ein offenes Tor wird gerne von unerwünschten Leuten genutzt, wenn sich dahinter etwas Begehrenswertes befindet. Selbst wenn das Begehren nur die reine Zerstörung ist. Welcher Port von welchem Dienst der DiskStations verwendet wird, kann man bei Synology nachlesen[9]. Die deutsche Synology-Community bietet außerdem in ihrem Wiki eine Liste[10] aller Ports mit einer Sicherheitseinstufung und weiteren Hinweisen an. Eine weitere Firewall findet sich ebenso in der DS, welche es jedoch schwerer hat zwischen Internet und LAN (lokalem Netzwerk) zu unterscheiden.

1.5 Schicht 4: Transportschicht

Als nächstes geht es um die Aufteilung der Daten in Pakete und die letzten Vorbereitungen vor dem Transport. Was bedeutet das genau? Die Protokolle dieser Ebene machen sich die Eigenschaften der unteren Schichten zu Nutze um den Netzwerkverkehr in Pakete zu teilen und dabei Staus zu vermeiden. Denn genau wie auf einer einfachen Straße können auch in einem Kabel immer nur eine gewisse Menge Daten gleichzeitig fließen; alles darüber geht verloren und sorgt eventuell sogar für „Unfälle“.

[9] http://www.synology.com/enu/support/help-page.php?q_id=299
[10] http://synology-wiki.de/

1.5.1 TCP vs. UDP

Spätestens wenn Sie eine Portfreigabe erstellen möchten, werden Sie auf diese Abkürzungen stoßen. Beide Protokolle gehen ein gemeinsames Problem mit zwei komplett unterschiedlichen Ansätzen an.

TCP setzt auf dem IP-Protokoll. Wenn es mit der Arbeit beginnt, baut es zunächst eine Verbindung zwischen den beiden Endpunkten auf - anhand seiner IP. Dann kann der Datenverkehr in beide Richtungen gleichzeitig erfolgen. Zumindest für die Augen des Programmierers, denn physikalisch ist das natürlich schwer realisierbar. Der Transfer lässt sich daher in zwei verschiedene Datenströme zerlegen, je einen pro Richtung. Meist fließen in eine Richtung die Daten und in die andere vorwiegend Steuersignale und Checksummen zur Überprüfung der Unversehrtheit.

Übrigens befinden wir uns hier immer noch im Bereich des Betriebssystems, beziehungsweise der Treiber (je nach OS sind beide schwer trennbar). Bei Windows ist dafür beispielsweise die DLL-Datei[11] winsock.dll bzw. winsock32.dll verantwortlich. Unter Linux ist TCP im Kernel integriert.

Eine TCP-Verbindung ist also eindeutig durch ihre beiden Endpunkte in Form von IP-Adressen identifiziert. Auch wird stets ein Port angegeben um mehrere Anfragen gleichzeitig zu bewältigen. Eine Verbindung wird dann als „Socket“ bezeichnet.

Aber viel interessanter wird diese Theorie, sobald man UDP dagegen stellt.

UDP sucht sich die beiden Endpunkte ebenfalls anhand einer IP-Adresse und einem Port. Doch bei UDP wird nicht sichergestellt, ob die Daten ihr Ziel erreichen. Der Sender erhält keinerlei Bestätigung über den erfolgten Datentransfer, von seiner Unversehrtheit ganz zu schweigen. Dafür minimiert es den nötigen Verkehr – schließlich werden nun einige Informationen wie das Senden der Checksummen komplett überflüssig. Unter anderem das DNS-Protokoll setzt daher auf UDP. Auch Internettelefonie, besser bekannt als VOIP, setzt auf UDP, denn wen interessiert da schon ein verloren gegangenes Paket bei der doch recht großen Menge an Gesamtdaten – wichtig ist ein halbwegs stabiles Signal ohne große Zeitverzögerung. Und gerade letzteres kann von UDP verringert werden. Ein einzelner Paketverlust lässt sich womöglich mit einem menschlichen Ohr nicht mal erkennen.

Es ist wie mit einem Sportwagen: Deutlich schneller, aber auch unsicherer wenn man auf Schickschnack verzichten möchte. Am wichtigsten ist dieses Wissen für Entwickler, denn sie müssen den Verlust von UDP berücksichtigen und selbst entsprechende Kontrollmechanismen veranschlagen.

1.6 Schichten 5 und 6

Ab jetzt geht es nur noch um reine Anwendungssoftware. Während je nach System die Schichten 1-4 in Hardware, Treibern oder Betriebssystemen stecken und von diesen verwaltet werden, beginnt mit Schicht 5 die Welt der Applikationen. Doch damit beginnt auch die Vielfalt. Netzwerkanwendungen zu schreiben ist kein Hexenwerk und jeder kann selbst entscheiden wie er die Daten verarbeitet. Aber eines nach dem anderen.

[11] Eine DLL-Datei enthält ausführbaren Programmcode. Ein Programm kann eine solche Datei in den Arbeitsspeicher laden und dann ausführen. Solcher Code wird meist von vielen Programmen benötigt. Er wird also häufig genutzt und ist doch nur ein einziges Mal vorhanden. Unter Linux übernehmen diese Aufgabe Bibliotheken.

1.6.1 Kommunikationssteuerungsschicht

Dieser Kandidat für das „Unwort des Jahres“ enthält eigentlich alles was es zu wissen gibt. Eine stehende Verbindung – auch Sitzung genannt – wird hierdurch kontrolliert. Sobald ein Zugriff länger andauert als ein Webseitenaufruf ist eine „Standverbindung“ manchmal ganz sinnvoll. Beispielsweise Telnet benötigt diese Schicht unbedingt.

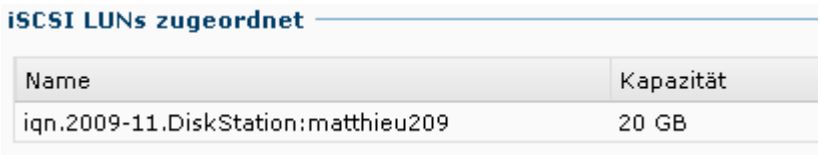
Doch ein Vertreter ist genau hier zu finden: iSCSI. Und damit wird schon der Unterschied zu anderen Protokollen sichtbar: SMB, AFP und andere sind in deutlich höheren Schichten angesiedelt und verschenken somit einige Performance.

1.6.1.1 iSCSI & CHAP

Diese netzwerkfähige Abwandlung von SCSI transportiert Daten zwischen einem Initiator, welcher die Verbindungsdaten festlegt, und einem Target (engl. Ziel). SCSI selber wurde für den PC-internen Gebrauch als Alternative zu ATA[12] konzipiert und dann als *internet small computer system interface* für den Netzwerkgebrauch umgestaltet. Windows unterstützt dies als Initiator bereits seit 2003 (Target ist nur mit einem Win-Server machbar), Mac nun seit 2008 ebenfalls. Die meisten Entwickler haben ihre Betriebssysteme bereits zwischen 2003 und 2005 entsprechend vorbereitet. Im Unterschied zu einer Netzwerkfreigabe ist iSCSI aufgrund seiner Geschichte deutlich tiefer ins System integriert. Statt zusätzlich gehandelt zu werden, stuft Windows es als normale Festplatte ein. Also können auch Programme darauf installiert und Formatierungen vorgenommen werden. Praktisch alles, was mit einer normalen Festplatte auch machbar ist.

Die optional verfügbare Verschlüsselung CHAP (*Challenge Handshake Authentication Pool*) ist als eine der sichersten zu betrachten. Durch besondere Kombinationen von Zufallswerten und Verschlüsselungen kann eine besonders hohe Sicherheit gewährleistet werden. Im Kern basiert das Verfahren auf einer Zufallszahl, welche zu Beginn erzeugt wird. Beide Seiten bilden anhand dieser Zahl einen Hashwert durch welchen sich der ursprüngliche Text nicht zurückverfolgen lässt (z.B. anhand von MD5-Checksummen).

Seit Version 3.0 unterstützt Synology noch weitere Funktionen[13]. So werden iSCSI-Targets jetzt in LUNs gespeichert. Auch hier kommt die Geschichte von SCSI zum Tragen. Ein LUN ist etwa vergleichbar mit einer virtuellen Festplatte. Ein Target liegt dann auf einem LUN vergleichbar mit einer Partition. Sind Sie soweit mitgekommen? Schön. So sieht das Resultat schließlich aus:



1.6.1.2 (My-)SQL

Recht häufig müssen Internetseiten auch größere Mengen von Daten erstellen und verwalten. Als Beispiel dienen dazu Online-Shops. Hierzu eignen sich am einfachsten Datenbanken. Das wohl bekannteste System ist SQL. SQL an sich ist allerdings kein Programm sondern nur ein Standard. Microsoft und andere Hersteller vertreiben verschiedene SQL-Server. Der beliebteste ist das kostenlose MySQL. Es bietet nicht zuletzt auch vergleichsweise hohen Komfort bei geringer Ressourcen-Nutzung. MySQL an sich kann ganz einfach aktiviert werden. Jedoch fehlt der DiskStation

[12] Software-Protokoll zur Steuerung und Nutzung von Massenspeichern in PCs, basierend auf IDE-Schnittstellen
[13] Nicht alle DS unterstützen die erweiterten Funktionen, etwa die x07-Serie sowie xxxj-Geräte.

jegliche Möglichkeit der Administration dieses Dienstes. Daher wird recht verbreitet PHPMyAdmin eingesetzt. Dieses kann extra über ein spk-Paket von Synology nachinstalliert werden. Intern verwendet Synology übrigens eine postgre-SQL-Datenbank für den DSM, da diese schlanker und schneller, jedoch schwerer zu handhaben und nicht für jeden Zweck bedingungslos nutzbar ist.

1.6.2 Darstellungsschicht

Doch viele Daten werden vor ihrem Versand noch einmal bearbeitet. Sei es komprimiert oder verschlüsselt oder …

Alle diese Verfahren gehören zur Schicht 6. Hier werden die Daten so vorbereitet, dass jedes System damit umgehen kann. Es werden also auch Zeichensätze wie ASCII umgesetzt um eine reibungslose Übertragung zu gewährleisten. Im Idealfall werden hier alle Abweichungen von Standards der unteren Schichten behoben. Doch auch Übersetzungsverfahren gehört zur Festlegung dieser Schicht, falls Daten einmal nicht in die Standards passen und eine „Notlösung“ gefunden werden muss.

1.7 Schicht 7: Anwendungsschicht

Und jetzt erst kommt die Anwendung selbst, welche ein Protokoll einsetzt um dann mit einem anderen Netzwerkteilnehmer zu kommunizieren. Die Liste an weiteren Unterpunkten wird daher jetzt sehr lang.

1.7.1 DNS & DDNS

Wer wöllte sich schon „173.194.69.113“ merken nur um zu Google zu kommen? Namen lassen sich nun mal für Menschen einfacher merken als Zahlenkolonnen (mit IPv6 würde das noch mal deutlich spannender). So gesehen ist DNS nicht unbedingt technisch notwendig; es schafft aber eine wichtige Brücke zwischen Mensch und Maschine.

Zum DNS-System gehören wie so häufig Client und Server. Die Anforderungen an Nameserver sind aber deutlich höher als für andere Anwendungen. So setzt zum Beispiel die für Deutschland und damit .de zuständige DeNIC („**De**utsches **N**etwork **I**nformation **C**enter“) drei, an getrennten Orten betriebene, Nameserver voraus bei denen man seine Domain hinterlegen lässt.

Zurück zur Funktionsweise: Im einfachsten Fall kontaktiert der heimische PC den Router (meist wird dieser per DHCP als DNS-Server vermittelt) und dieser dann (sofern er die Domain nicht im Zwischenspeicher[14] hat) den DNS-Server des Providers („ISP“). Man kann aber auch einen anderen DNS-Server in der Konfiguration von Betriebssystem und/oder Browser eintragen. Doch auch diese Server sind meist nicht für die Domain zuständig. Im DNS-Kontext gibt es stets ein paar wenige Server welche vom Inhaber autorisiert worden. Sie verschicken dann auch eine entsprechende Antwort. Alle anderen speichern die Ergebnisse nur zwischen und Fragen bei Bedarf neu an. In diesem Fall spricht man von einer „Nicht autorisierenden Antwort“ (non-authoritive). DNS-Abfragen lassen sich übrigens auch per Hand durchführen; Windows kennt dazu „nslookup“.

[14] Technisch korrekter wäre „Cache“

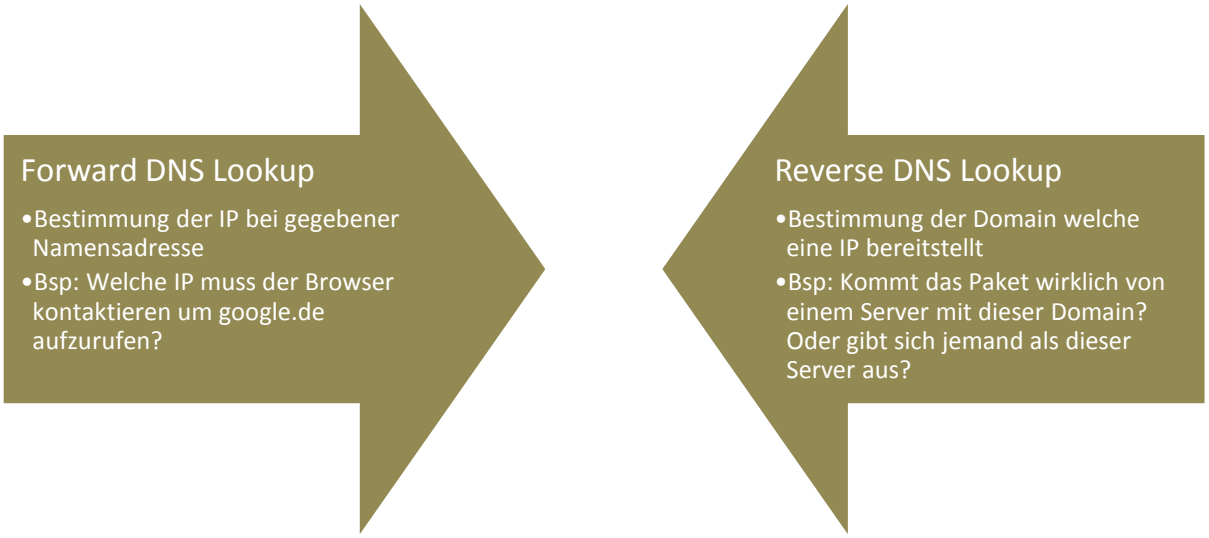
Wer schon einmal versucht hat, seine Disk Station von außen zu erreichen, wird mit einem weiteren Problem der IPv4-Adressen konfrontiert: Moderne DSL-Zugänge wechseln ihre IP-Adressen regelmäßig. Selbst wer nun sagt, dass er seinen Router nie vom Netz trennt und daher ja keine neue IP bekommen kann, irrt sich. Mindestens einmal pro Tag wird der Router „Zwangs-Neu-Verbunden“. Nur wenige Provider nutzen von Haus aus feste IP-Adressen. Bei den meisten ist dies als nicht gerade günstige Option zusätzlich buchbar. Die Zwangstrennung dient übrigens der Optimierung der DSL-Frequenzen; ohne würde die Datenrate nach mehreren Tagen wahrscheinlich immer weiter nachlassen.

Der Ursprung dieses Problems liegt im IPv4-Protokoll, welches die Adressen in einem Netzwerk vergibt. Zwar gibt es seit über einem Jahrzehnt bereits den Nachfolger IPv6, doch aufgrund der unterschiedlichen technischen Grundlagen ist ein Umstieg für die Provider ein nicht zu unterschätzender Kraftakt. Auch Software müsste im Falle einer Änderung angepasst werden. IPv4 hat zu wenig mögliche Adressen, weshalb die Provider dynamisch vorgehen müssen um keine Bereiche zu verschwenden.

Um einen Weg aus dieser Krise zu finden, gibt es DDNS. Das Kürzel „D“ steht für „dynamisch“. Heraus kommt eine dynamische Namens-Adresse. Anbieter für dieses System gibt es einige. Bei den kostenlosen Anbietern wie dem amerikanischen „dyndns.org“ muss man allerdings mit der Einschränkung leben, nur eine Sub-Domain zu besitzen (z.B. http://meine.dyndns.org). Wer dagegen bereit ist, ein wenig Geld auszugeben, kann preiswert sogar eine echte .de-Domain bekommen. (z.B. bei selfhost.de).

1.7.1.1 Forward & Reverse DNS

Bei DNS-Abfragen muss man prinzipiell zwei verschiedene Möglichkeiten unterscheiden. Zum einen: Wie heißt die IP hinter einer Adresse, zum anderen wie heißt der Name zu einer IP. Letzteres ist gerade für Mail-Server interessant. Nur wer sich auch in diese Richtung genau einer Adresse zuordnen lässt ist häufig wirklich Absender. Viele Mailanbieter werfen Nachrichten bei denen ein solcher „Reverse“-Lookup fehlschlägt einfach weg.



1.7.1.2 Zone vs. Domain

Die „Zonen" eines DNS-Systems habe ich bisher etwas vermieden, doch wenn man sich mit dem DNS-Server einer Synology beschäftigen möchte, kommt man um diese Begriffe nicht herum. Grundlegend repräsentiert eine Domain einen kompletten Weg durch die Baumstruktur des DNS, während eine Zone nur für einen Teil dieses Pfades steht. So ist „.org" eine Zone, während „example.org" eine vollwertige Domain ist (auch FQDN genannt, „Full Qualified Domain Name". Für diese sind aber eben zwei Zonen notwendig: „.org", und „example" innerhalb von „.org". Für eine solche Zone ist immer ein bestimmter DNS-Server (Nameserver) zuständig. Nur er, sowie vom Anbieter/Inhaber bestimmte (optionale) Slave-Server dürfen autorisierte Antworten ausliefern. Im schlimmsten Fall müssen also für eine Domain mit 4 Ebenen (z.B. „eins.zwei.example.org") auch 4 Zonen ausgewertet werden.

1.7.1.3 Eine Zone im Detail

Alle Angaben an dieser Stelle sind frei erfunden und liegen in dieser Form auf keinem DNS-Server! Sie dienen nur zur Veranschaulichung.

```
example.com.  IN  NS    ns1.example.com.  ; Zonefile for example.org
@             A         78.47.214.74
www           A         78.47.214.74
@             AAAA      2a01:4f3:3f9:::1
ftp           CNAME     www
@             MX 10     mail
```

Zugegeben, auch das ist keine vollständige Zonen-Datei. Denn eine solche würde noch ein klein wenig mehr Informationen enthalten, die aber eher für den DNS-Server relevant sind. Mir geht es an dieser Stelle vor allem um ein paar verschiedene Möglichkeiten die in diesem kurzen Beispiel wohl gut ankommen dürften.

Ganz wichtig: Leerzeilen sind in einer Zonendatei eigentlich unzulässig. Auch wenn das der ein oder andere Server akzeptieren mag, richtig ist es nicht.

Alles was hinter einem „;" steht, ist ein Kommentar. Die erste Zeile wird daher nur zur Hälfte interpretiert. In der ersten Hälfte muss außerdem der Eintrag „IN" vorhanden sein.

Außerdem gilt, dass „@“ stets für den Namen der Zone gilt. Man könnte im obigen Beispiel auch jedes Mal „example.org.“ eintragen. Die folgenden Einträge sind meist die wichtigsten in einer solchen Datei und sind auch oben verwendet:

A – Ipv4-Adresse

AAAA – Ipv6-Adresse

NS – Zuständiger DNS-Server. So können darunter liegende Zonen an andere DNS-Server verwiesen werden.

CNAME – Anweisung, die IP einer anderen Domain zu nutzen

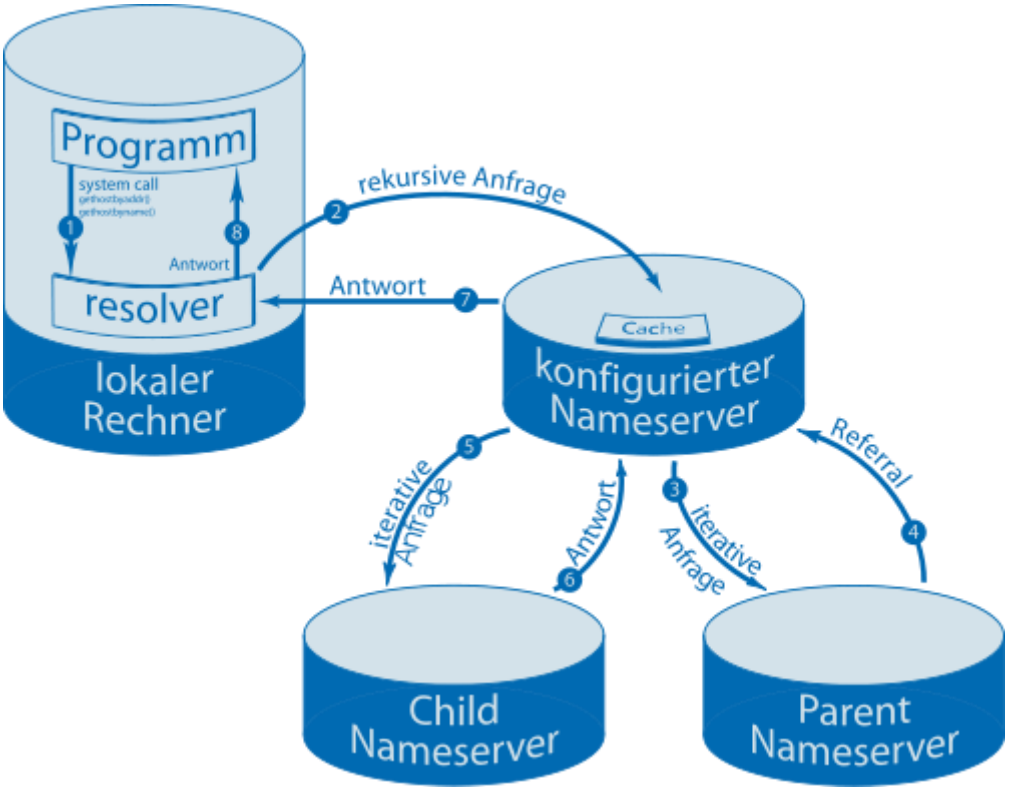
MX – Mail-Server

1.7.1.4 Rekursiv und iterativ

Eine nicht-autoritative DNS-Abfrage kann diese beiden Betriebsmodi nutzen. Viele Clients können aber nur mit rekursiven Anfragen arbeiten.

Bei einer rekursiven Anfrage bekommt der Client die verlangte Antwort direkt. Da in den überwiegenden Fällen DNS-Server diese Antwort aber nicht sofort kennen, befragen Sie wiederum andere Server. Diese sind dann iterative Anfragen.

Aber wie so oft sagt ein Bild mehr als Worte:



Quelle: http://de.wikipedia.org/wiki/Datei:Dns-abfrage.svg (Lizenz: Creative Commons-by-sa)

1.7.2 http/https

Nachdem eine Verbindung zwischen den beiden Geräten aufgebaut wurde, tritt ein anderes Protokoll in Kraft um Daten zu übertragen. Im Falle von Webseiten ist dies meistens http. Das *hyper-*

Text-Transfer-Protokoll bietet eine große Vielfalt der möglichen zu übertragenden Medien. So kann es einfachen Text genauso bereitstellen, wie Farben, Bilder oder auch ganze Dateien. In den DiskStations kommt http beim Webserver, welcher über http://DiskStation/ erreicht werden kann, und bei der Administration über das Interface (http://DiskStation:5000) zum Einsatz. Hinter dem Doppelpunkt werden Ports angegeben. Zu diesen möchte ich aber später mehr sagen. Der größte Nachteil des http-Protokolls ist die fehlende Verschlüsselung und somit geringe Sicherheit. Dies bringt uns zu https. Hier wird die gesamte Übertragung verschlüsselt und sollte damit erste Wahl für wichtige Informationen, wie Passwörter oder persönliche Informationen sein. Synology-Produkte lassen sich so ansprechen, indem wir einfach das „http“ am Anfang gegen „https“ eintauschen (https://DiskStation/). Während der Browser weiß dass er nun von Standard-Port 80 auf 443 springen muss, ändert sich bei Anwendungen außerhalb der Standard-Ports der Port wie beispielsweise für den DSM[15]: https://DiskStation:5001/. Aufgrund der Verschlüsselung dauert die Übertragung natürlich etwas länger, doch dank der Geschwindigkeit heutiger Internetverbindungen und aktueller Computer ist dieser Unterschied fast nicht mehr auszumachen. Wer auf seiner DiskStation Webseiten betreibt, welche sensible Daten wie Passwörter oder persönliche Informationen übertragen, sollte daher ausschließlich https verwenden.

1.7.3 FTP (File-Transfer-Protokoll)

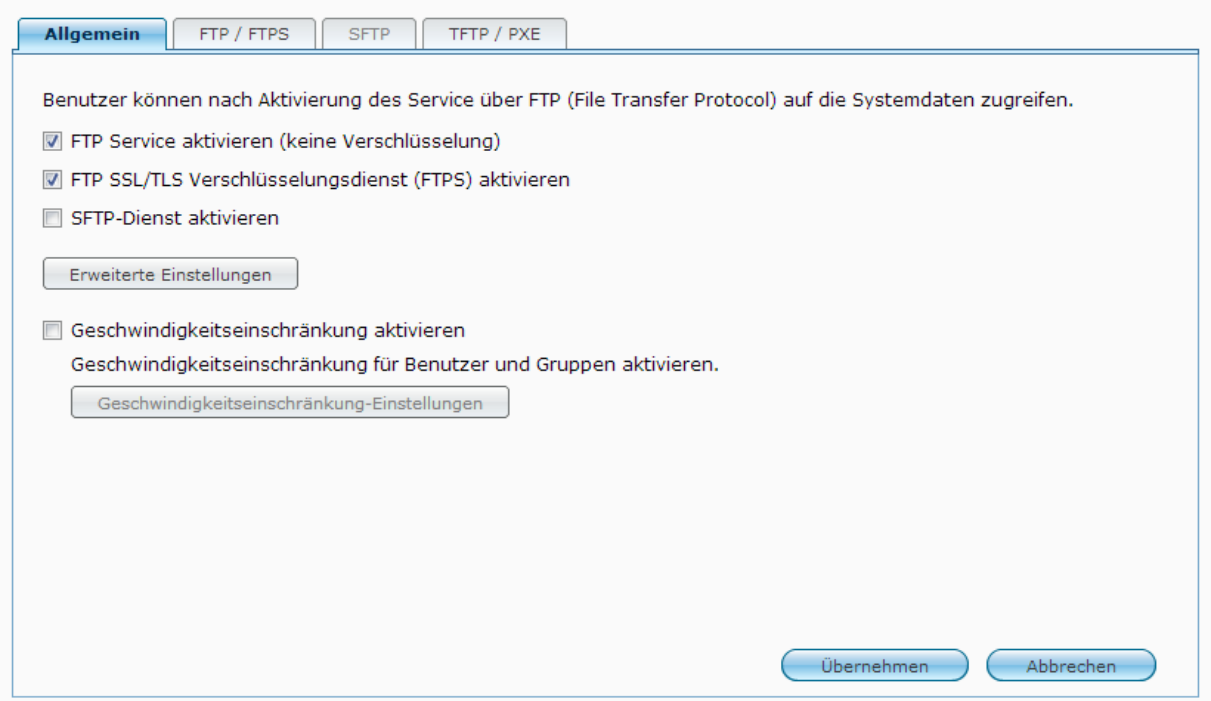
Im Gegensatz zu http, kann ftp keine Internetseiten übertragen. Seine Stärken liegen in der Übertragung von Dateien. Während http ein „Allround-Talent“ ist und daher keine besonders guten Geschwindigkeiten bei Downloads erreichen kann, holt ftp deutlich mehr aus dem möglichen heraus. Die meisten gängigen Browser unterstützen das FTP-Protokoll und liefern über ftp://DiskStation/ meist einen Überblick über ihre Dateien. Benutzername und Passwort werden hier im Klartext in die URL integriert: ftp://user:passwort@DiskStation. Doch dies ist generell sehr Text-orientiert und unübersichtlich. Daher sind separate Programme, wie die frei erhältlichen WinSCP und FileZilla deutlich besser für diese Zwecke geeignet. Diese Programme bieten eine Windows-Explorer-ähnliche Oberfläche und machen den Dateitransfer per simplen Drag-und-Drop möglich.

Zusätzlich muss man bei FTP noch zwischen aktiver und passiver Übertragung unterscheiden. Vereinfacht gesagt: Während beim passiven FTP die Übertragung über Port 21 gesteuert wird und der Datenverkehr einen speziellen Portbereich beansprucht, kontaktiert ein Client beim aktiven FTP zunächst den Server auf Port 20 und teilt ihm dann einen anderen Port mit, welchen er für die Kommunikation verwenden wird. Doch das ist recht vereinfacht. Im Internet finden sich vielfältige Erklärungsversuche[16] in dieses komplexe Thema.

Doch ähnlich wie http, hat auch ftp mit der fehlenden Sicherheit zu kämpfen. Aufgrund der fehlenden Verschlüsselung braucht man nur den Internetverkehr mitzuschneiden und kann dann recht einfach die Anmeldedaten auslesen und missbrauchen. Die Lösung heißt sftp. Dieses Protokoll nutzt als Grundlage SSH (womit wir uns als nächstes beschäftigen) und dessen Verschlüsselung um auf Dateien zuzugreifen. Daneben gibt es noch die Varianten „FTPS“ und „TFTP“. Ersteres verwendet eine andere Verschlüsselung und letzteres ermöglicht einen sehr einfachen Zugriff auf FTP-Ressourcen. Wozu das gut ist wird beim Thema „PXE“ deutlich.

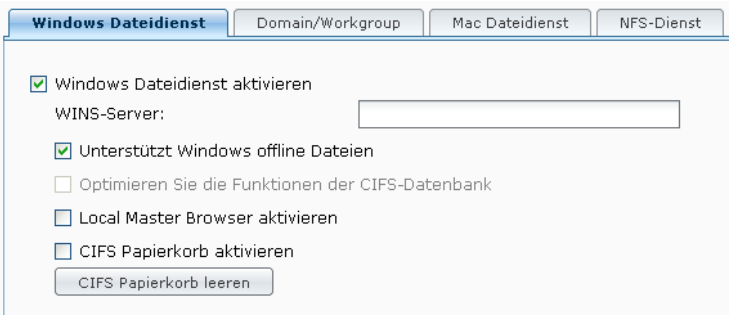
[15] DSM = DiskStation Manager, Web-Administrationsoberfläche
[16] Z.B.: http://slacksite.com/other/ftp.html

Wegen der besseren Ausnutzung der Verbindung sollten sie immer als Download-Link für ihre Benutzer ftp statt http nutzen. Ein Beispiel für die längeren Zeiten ist die Nutzung der FileStation, welche auf http statt ftp setzt.



1.7.4 SMB/CIFS

Die Server Message Block genannte Technologie wurde erstmals 1983 durch einen IBM-Mitarbeiter vorgestellt. Microsoft nutzte zunächst das eigene NetBIOS als Grundlage statt TCP/IP. Doch aufgrund der zunehmenden Verbreitung dieser beiden Standards sah man sich gezwungen, SMB zunächst über ein TCP/IP-basierte NetBIOS anzubieten und schließlich auch direkt auf TCP/IP-Basis. Später beteiligten sich immer mehr Firmen an der Erweiterung des Protokolls. Auf Druck der Europäischen Union legt Microsoft seit 2007 aber alle Spezifikationen offen. Der Entdeckung dieser Geheimnisse hat sich später auch das Samba-Team verschrieben, welches den gleichnamigen Server programmiert. Dieser kommt bei jeder DS für gleich mehrere Protokolle zum Einsatz. Auch der FTP-Server ist mit dem Samba eng verbunden um das Berechtigungsmanagement so einfach wie möglich zu halten. Mittlerweile wird Samba offiziell von Microsoft gefördert, was mittlerweile sogar eine ActiveDirectory-ähnliche Funktionsweise ermöglicht hat.



1996 wurde dann CIFS (Common Internet File System) eingeführt. Die stark erweiterte Version von SMB zeichnete sich insbesondere durch Integration von NT-Domänen und anderen typischen Windows-Funktionen aus. „Common Internet“ ist aber eine reine Übertreibung. Man sollte CIFS (wie auch SMB) auf keinen Fall über das eigene Netzwerk hinaus betreiben.

Mit neueren Windows-Versionen folgten dann SMB 2.0 (Win Vista), 2.1 (Win 7) und 3.0 (Win 8).

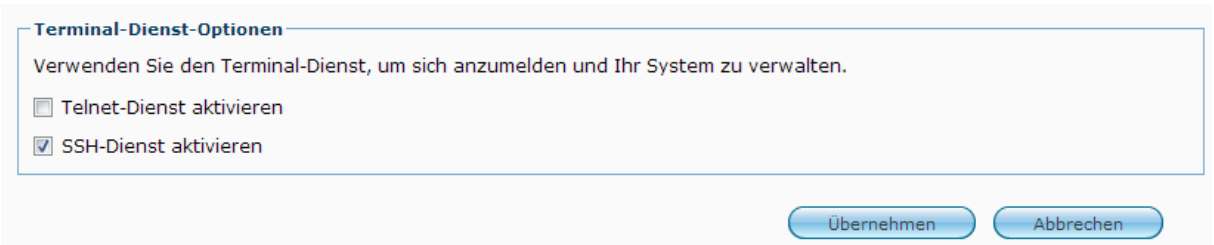
1.7.5 WebDAV

FTP stellt Dateien bereit, benötigt einen eigenen Client und ist schwierig zu konfigurieren (wenn man nicht ein vorkonfiguriertes System wie eine DiskStation verwendet). Eher suboptimal wenn man in einem Team einfach nur Daten kooperativ nutzen möchte.

HTTP ist die Basis der Alternative WebDAV. Es fügt jedoch Versionsverwaltung und einiges mehr hinzu. Das ursprüngliche Ziel war die Bearbeitung von Webpräsenzen zu koordinieren. Daher auch die http-Auslegung: WebDAV ist so (theoretisch) recht einfach in den Webserver integrierbar. Auch der Port 80 wird hier verwendet. Eine Firewall ist also kein Problem, wenn man nicht den gesamten Zugriff auf Webseiten kappen möchte. Ähnlich wie FTP arbeitet auch WebDAV über Steuersignale

1.7.6 Telnet/SSH

Telnet stammt aus der Zeit von Unix und wird verwendet um auf andere Rechner per Remote (engl. Fernbedienung) zuzugreifen. Der Nutzer arbeitet dann in einer sogenannten Shell, welches ein Textfenster mit meist weißer Schrift auf schwarzem Hintergrund darstellt. Wer derartige Technologien für veraltet hält, dem sollte gesagt sein, dass Microsoft in Windows 7 sich, nachdem man der hauseigenen Shell schon den Rücken gekehrt hatte, wieder zum standardmäßigen Einbau entschlossen hat, damit Netzwerkadministratoren direkt auf andere Windows-Rechner im Netzwerk zugreifen können, ohne durch die ganze Firma zu rennen. Diese Technologie beherrscht natürlich auch der UNIX-Abkömmling Linux, welcher auf den Synology-Produkten eingesetzt wird. Auch für Telnet gibt es unter Windows wieder einen Client, der einem die Arbeit erleichtert. Der am stärksten verbreitete Client ist das kostenfreie Putty. Linux-Benutzer können in eine Textaufforderung über das Kommando „user@IP“ eine Verbindung aufbauen. Dazu geben sie die Adresse des zu kontrollierenden Gerätes ein, wählen die Verbindungsart (Telnet, SSH, …)(belassen den Port bei 22 bzw. 23) und bestätigen. Nach ein paar Sekunden sollten sie dann das beschriebene, simple Fenster sehen. Zuerst werden sie nach dem Benutzernamen gefragt. Aus Erfahrung würden sie hier natürlich „admin“ eintragen. Doch wer schon mal mit Linux gearbeitet hat, weiß, dass der Nutzer mit den meisten Rechten hier „root“ heißt. Das Passwort unterscheidet sich allerdings nicht von dem des „admin“. Was genau sie nun machen können, werden wir später erörtern. Wer trotzdem schon mal sehen will, was alles so möglich ist, tippt „help“ in die Konsole. Seien sie allerdings vorsichtig, denn sie arbeiten nun im absoluten Kern des Betriebssystems. Ein falscher Befehl und Ihr System ist hinüber. Aus genau diesem Grund ist es sehr gefährlich, wenn Eindringlinge auf diesem Weg Zugriff auf ihr System bekommen. Insbesondere Telnet hat mit äußerst hohen Sicherheitsproblemen zu kämpfen, da es keine Verschlüsselung einsetzt und die gesamte Übertragung im Klartext erfolgt. Aus diesem Anlass heraus wurde SSH entwickelt. Diese *Secure Shell* verschlüsselt effektiv den gesamten Verkehr. **Daher sollte man NIE über Telnet aus dem Internet auf seine DiskStation zugreifen.** Deshalb mein Rat: Lassen sie die Option für Telnet immer aus und nutzen Sie stattdessen SSH. Dieses Mal geht es nicht nur um ihre Daten, sondern um ihre gesamte DiskStation. Natürlich muss dabei auch wieder ein anderer Port verwendet werden. Standardmäßig ist das die 23.



1.7.7 POP3, SMTP, IMAP

Diese drei Protokolle werden von uns jeden Tag genutzt. Aber im Gegensatz zu http, fällt uns das nicht jeden Tag ins Auge. Denn einmal konfiguriert, läuft alles automatisch. Die Rede ist von E-Mail-Protokollen. In der DiskStation werden sie von der Mail Station verwendet, welche als spk-Paket bei Synology vorliegt und einfach mit einem Klick installiert werden kann[17]. Die bekanntesten sind POP3, IMAP und SMTP und werden auch von der Mail Station in vollem Umfang unterstützt.

Zunächst zum *Post Office Protocol* in Version 3.0 oder kurz POP3. Dieser Vertreter beschränkt sich rein auf das Abholen von Mails. Genauer genommen unterstützt es das Auflisten, Abholen und Löschen der Mails, bietet aber keine Möglichkeit des Sendens und muss daher immer im Verbund mit einem anderen Protokoll genutzt werden. Standardmäßig verwendet POP3 den Port 110, wobei auch die Mail Station keine Ausnahme ist. Wer also auch außer Haus dieses Protokoll nutzen möchte, wird um eine entsprechende Portfreigabe nicht herumkommen. Die erste Version wurde bereits 1984 veröffentlicht und es dauerte nur ein Jahr, bis die zweite Version folgte. 1988 fand dann die endgültige Version 3 seine Endfassung. Die meisten gängigen Mail-Clients unterstützen POP3.

Die Übertragung von Daten erfolgt allerdings, ähnlich wie bei FTP und HTTP, komplett unverschlüsselt und im Klartext, wodurch es sehr anfällig für Sicherheitsrisiken ist. Dafür wurde POP3S geschaffen, welches über Port 995 kommuniziert und SSL/TLS für die Verschlüsselung nutzt, also ebenfalls vergleichbar mit dem von der DiskStation verwendeten *FTP over SSL/TLS*. Auch gibt es verschiedene Ansätze für serverseitige Sicherung, doch dort konnte sich keine Software bisher durchsetzen.

Als nächstes zu IMAP oder *Internet Message Access Protocol*. Als Portnummer wurde hier 143 registriert. Auch IMAP kennt verschiedene ältere Versionen, welche aber nicht mehr genutzt werden, weshalb eine Unterscheidung nicht nötig ist. Die Entwicklung begann 1986 mit dem Ziel, alle Nachrichten so bereitzustellen, als ob die Mails direkt auf dem Rechner liegen würden. Im Gegensatz zu POP3, bleiben die Mails komplett auf dem Server und werden nicht heruntergeladen. Gemeinsam hat es allerdings die Eigenschaft, keine Mails versenden zu können. Dass die Mails auf dem Server bleiben, hat aber noch andere Nebenwirkungen. So ist der Netzwerkverkehr recht hoch und da beispielsweise die Suche vom Server erledigt werden muss, bedeutet jenes auch für unsere DiskStation mehr Arbeit.

Wie bereits POP3, verwendet auch IMAP standardmäßig keine Verschlüsselung. Stattdessen muss die Verbindung über Port 993 gelenkt werden um eine Verschlüsselung über SSL zu gewährleisten. Man sollte die Verwendung von IMAP auf der eigenen DiskStation allerdings gründlich abwägen, aufgrund des bereits angesprochenen höheren Netzwerkverkehrs und der gesteigerten Leistungsanforderungen.

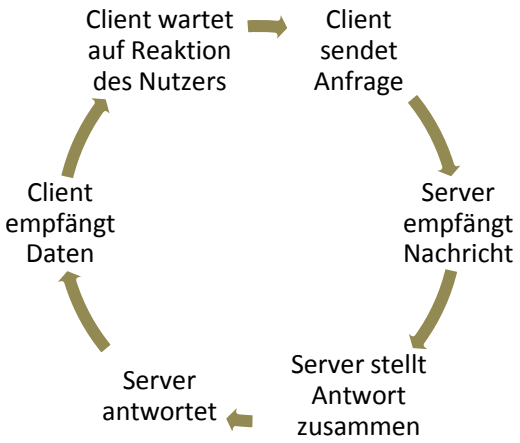
SMTP ist auf der DiskStation die einzige Möglichkeit, Mails zu versenden. Leider ist auch dem *Simple Mail Traffic Protocol* seine mehr als 20-jährige Geschichte anzumerken. Es verwendet Port 25 und bietet leider keine Möglichkeit der Verschlüsselung. Unglücklicherweise bietet die Mail Station sogar die Möglichkeit, das größte Problem an SMTP unkorrigiert zu lassen. Denn standardmäßig sieht SMTP nicht einmal vor, dass sich die Nutzer mit Benutzername und Passwort authentifizieren müssen.

[17] Download: http://synology.de, anschließend Installation über das „Paketmanagement“ im DiskStation Manager

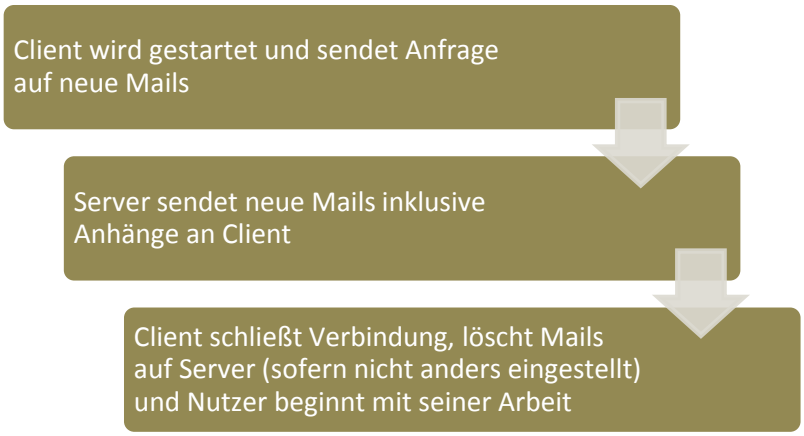
Diese Funktion wurde später hinzugefügt. **Man sollte daher immer den entsprechenden Haken in der Mail Station setzen!**

Wer sich allerdings gar nicht erst mit Portweitergaben und Protokollfragen herumschlagen möchte, lässt die Ports einfach geschlossen und verwendet stattdessen den RoundCube-Webmail-Client, welcher unter http://DiskStation/mail erreichbar ist. Noch besser ist natürlich die Verwendung von https. Für RoundCube muss nur IMAP aktiviert sein.

Hier noch einmal zwei Grafiken, welche den Unterschied zwischen POP3 und IMAP verdeutlichen sollen:



-> IMAP



-> POP3

1.7.8 UPnP

Nun zu einem anderen Thema: Medienfreigabe.

Synology verwendet dabei ein Protokoll namens *Universal Plug and Play* oder kurz „UPnP“. Dieser Standard ermöglicht es, herstellerübergreifend, Geräte über ein IP-Netzwerk kommunizieren zu lassen. UPnP zeichnet sich durch hohe Flexibilität und Vielseitigkeit aus. So beschränkt es sich nicht nur, wie man zunächst annehmen könnte, auf PC-Netzwerke, sondern kann auch über jeden anderen IP-fähigen Kommunikationsstandard genutzt werden. So kommt es, dass mittlerweile auch UPnP über Bluetooth, WLAN und sogar FireWire genutzt werden kann.

Ein typisches UPnP-Netzwerk baut sich meist wie folgt auf:

NAS
- Speichert Dateien, welche bereitgestellt werden sollen
- z.b.: Eine Synology DiskStation

PC
- Zugriff auf andere Geräte und zentrale Steuer-Funktion
- Kann Rolle anderer Geräte übernehmen: Sowohl als Dateispeicher, Fernbedienung als auch Abspielgerät

Fernbedienung
- Wiedergabe anderer Geräte kontrollieren
- z.b.: Spezielle Multifunktionsfernbedienung, Handy oder PDA

UPnP-fähiges Abspielgerät
- Ruft Dateien ab und gibt diese über angeschlossene Geräte (z.b. Fernseher oder Stereoanlage) wieder

Eine DiskStation nimmt dabei also die Rolle eines Datenspeichers ein. Das wohl bekannteste „Abspielgerät“, welches von Synology auch als solches ausgewiesen und als kompatibel angegeben wird, ist die Sony Play Station 3. Doch der UPnP-Server der DiskStation sollte auch mit den meisten anderen Geräten problemlos kooperieren, insofern dort der UPnP-Standard lückenlos und korrekt implementiert[18] wurde.

Mit der Funktion „Medien-Renderer“ in der Audio Station kann eine DS nun auch als Fernbedienung dienen.

Um Kontakt aufzubauen, wird der DHCP-Dienst verwendet, welcher zunächst IPs verteilt. Als nächstes „schreit“ das Gerät seine Informationen quer über das Netzwerk, in der Hoffnung auf möglichst viele Antworten. Standardmäßig wird hierzu UDP verwendet. Für jede Adresse welche als Antwort erhalten wurde, werden nun so viele Informationen wie möglich gesammelt. Dazu lädt sich das Gerät von jeder Gegenstelle eine XML-Datei.

[18] Implementieren – Bezeichnet in der Programmierung die vollständige Umsetzung sowie Veröffentlichung eines Features / einer Funktion.

Damit ist eine Verbindung hergestellt und das Gerät kann nun auf Abruf seinen Dienst bereitstellen. Das erfolgt zum einen, über Nachrichten welches es über das Netzwerk sendet und zum anderen über Nachrichten welche von anderen Geräten empfangen werden, sollte sich etwas im Netzwerk verändert haben.

1.7.9 DLNA

Die DLNA ist eine Vereinigung von Firmen, welche einen einheitlichen Standard für die Netzwerk-Kommunikation insbesondere zur Medien-Freigabe schaffen möchte. Die „Digital Living Network Alliance“ wurde im Jahre 2003 von Sony und Intel gegründet und veröffentlichte ein Jahr später seine ersten Richtlinien, womit die offizielle Arbeit beginnen konnte. Mittlerweile gehören ihr nach eigenen Angaben[19] mehr als 230 Unternehmen an, welche eigene Produkte registriert und zertifiziert haben.

Mit dem DSM 2.2 kam auch ein DLNA-Medienserver auf die DS. Somit ist eine reibungslose Kommunikation mit anderen zertifizierten Geräten beinahe[20] garantiert. Auch neue Funktionen wie ein „on-the-fly-konvertieren“, also konvertieren während abgespielt wird, sind nun Teil des Medienservers.

1.7.10 LDAP

Windows-Administratoren kennen mit “Active Directory” eines der zahlreichen LDAP-Systeme. LDAP selbst ist ein festgelegter Standard zur Kommunikation zwischen Client und Server – Implementationen, also Umsetzungen dieser Technik, gibt aber es viele. Außerdem gehört zu LDAP auch eine Datenbank in der alle Informationen gespeichert werden. Diese Datenbank wird gemeinhin als „LDAP-Verzeichnis“ bezeichnet, die Kommunikation als „LDAP-Protokoll“.

Am häufigsten wird LDAP daher auch zur Authentifizierung von Benutzern verwendet. Betriebssysteme der Unix-Familie (u.a. Linux und Mac OS) können meist von Haus aus LDAP-Server ansteuern. Windows tut sich etwas schwer, kann über zusätzliche Anwendungen aber selbiges. Doch auch für Adressbücher und ähnliche Anwendungen ist die zugehörige Datenbank überaus geeignet. Doch diese Funktionen spielen im Zusammenhang zu einer DiskStation keine Rolle, denn der von Synology verwendete LDAP-Server nutzt als Datenbank die eigenen Informationen der hinterlegten Benutzer und Passwörter und kann daher nicht mit Adressdaten und ähnlichem umgehen.

In langer Form heißt LDAP übrigens „Lightweight Directory Access Protocol“. Das LDAP-Protokoll ist aktuell in dritter Version veröffentlicht (LDAPv3) und existiert ursprünglich seit 1993.

Eine LDAP-fähige-Datenbank ist hierarchisch aufgebaut und besteht somit aus Wurzeln, Zweigen und Blättern. Die Wurzel bildet dabei eine Organisation, in der Datenbank mit „o“ abgekürzt. Wie es danach weitergeht, unterscheidet sich je nach Datenbank. Gebräuchlich wäre aber beispielsweise ein solcher Pfad:

uid=MaxMuster,ou=raumschiffe,ou=vertrieb,c=at,o=Intergalaktik

An diesem Beispiel wird deutlich, dass sich im Pfad „aufwärts“ also in Richtung Wurzel bewegt wird und nicht umgekehrt wie es manchmal vielleicht praktischer wäre. Das Unternehmen (hier „Intergalaktik“) steht daher zuletzt. Jedes Element steht für einen Zweig, das erste („uid“) für das

[19] Quelle: http://www.dlna.org/about_us/about/, Stand Februar 2013
[20] DLNA selbst legt leider nur wenige Formate fest, daher ist es von der Gnade der Hersteller abhängig, welche Video- und Musikdateien (Codecs) genau funktionieren.

Objekt. Die Abkürzungen bedeuten in diesem Fall: „uid“=User ID, „ou“=Organizational Unit / Organisationseinheit, „c“=Country / Land. Es gibt aber auch andere Schreibweisen. Zum Beispiel kann man mit der Organisation beginnen und dann in der Organisation herabsteigen bis man bei dem einzelnen Benutzer angelangt ist. Dann entfallen aber auch die Abkürzungen und als Trennung wird ein „/“ verwendet.

Zu dem bisher beschriebenen kommen dann noch Attribute und Klassen die Daten enthalten oder zuordnen.

Das LDAP-Protokoll wirkt dagegen fast schon primitiv einfach und beschreibt, wie Anfragen an den Server aussehen müssen. In einer solchen Anfrage muss definiert sein wonach man sucht, mit welchem Account und wo mit der Suche begonnen werden soll (alles in der Hierarchie oberhalb dieses Punktes wird dann nicht durchsucht).

1.8 Programmiersprachen und Co

1.8.1 html

Der Urvater des Webs, Tim Berners Lee, erfand höchst persönlich diese Sprache welche noch heute Grundlage von Webseiten ist. Eine Programmiersprache im klassischen Sinne ist html jedoch nicht, da nicht wie üblich der Quelltext in binärem Code oder vergleichbares umgewandelt wird, sondern ist selbst eher ein Webersatz für binären Code. PHP und andere Anwendungen wandeln ihre Skripte in html um, da Browser mit PHP nicht viel anfangen können.

Wir sind damit jetzt also nicht mehr bei den Protokollen selbst sondern bei dem was sie übertragen. Wenn ein Nutzer eine Seite anfordert, dann wird ein sogenannter Request abgesetzt den dann bei Internetseiten meist http beantwortet und an seine Antwort gleich die entsprechende Datei anhängt. Jetzt muss nur noch der Empfänger das interpretieren, was er jetzt erhalten hat und schon kann der Nutzer wieder in Aktion treten und den Browser die nächsten Meldungen absetzen lassen.

html ist recht simpel aufgebaut. Die Befehle werden genauso angegeben wie sie später in Form von Text und Bild (und beim neuen html 5 dann auch als Musik und Videos) wiedergegeben werden sollen. Jeder Browser geht dabei ein wenig anders vor, weshalb eine Standard-konforme Verwendung wichtig ist um Problemen vorzubeugen[21]. Somit wird die „Hypertext Markup language“ auch zu den Auszeichnungssprachen gezählt da es „nur“ Objekte textbasiert platziert und anschließend wieder zusammensetzt. Seit seiner ersten Implementierung 1989 hat html eine lange Entwicklung durchgemacht und soll bald in Version 5 erscheinen welche es dann Web-2.0 geeignet machen soll, unter anderem durch einen <video>-tag der Multimediainhalte ohne Player (Flash, …) wiedergeben soll.

1.8.2 PHP

Dort wo html aufhört, macht PHP weiter. Es bietet sehr flexible Möglichkeiten zum Erstellen dynamischer Internetauftritte. Auf der anderen Seite kann PHP kein html ersetzen. Im Gegenteil: PHP kann nicht von Browsern interpretiert werden, da viele Informationen welche PHP nutzt, nur für den Server (in unserem Fall unsere DiskStation) zugänglich sind. Bevor die Seite daher übertragen wird, wandelt der Server den PHP-Code in normale html-Seiten um. Trotzdem kann PHP ganz einfach mit html in einer Datei eingesetzt werden, ohne das eine neue Datei benötigt wird. Die Macher von PHP vereinen in ihrem Konzept die Vorteile von JavaScript (einfach zu erlernen, in selber Datei

[21] Das W3C-Konsortium hat dafür einen eigenen „Validity Check“ geschaffen: http://validator.w3.org/

verwendbar) und Perl (vielfältige Möglichkeiten, teilweise aber sehr kompliziert). Auf unserer DiskStation bietet PHP neben vollen Linux-Programmen die einzige Möglichkeit mit Datenbanken zu arbeiten. Es wird außerdem frei entwickelt und besitzt keine Lizenzkosten. Auch ist es für Einsteiger schnell zu erlernen und trotzdem sehr leistungsfähig. Der Webserver der DiskStation unterstützt PHP nach Aktivierung ohne Probleme. Aus Sicherheitsgründen müssen einige Funktionen jedoch explizit aktiviert werden. Auch lasst sich dort ein Cache aktivieren der dynamische Seiten statisch speichert um Last und Antwortzeiten zu minimieren. Bei Seiten mit viel dynamischem Inhalt kann dies sowohl von Vorteil sein, als auch Probleme schaffen wenn Daten nicht mehr ausreichend neu berechnet werden und Nutzer daher falsche oder fehlerhafte Seiten angezeigt bekommen. Bei Problemen mit eigenen Seiten und CMS[22] sollte daher diese Funktion testweise deaktiviert werden. Einige CMS bringen auch eigene Cache-Systeme mit.

1.8.3 RSS

Obwohl es eigentlich, technisch gesehen, nur eine XML[23]-Seite ist, wird der RSS-Standard immer wichtiger und immer mehr Menschen nutzen ihn um über die neuesten Ereignisse im Bilde zu sein.

Um Daten abzugleichen, funktioniert ein abonnierter RSS-Feed fast wie ein E-Mail-Programm. In regelmäßigen Abständen gleicht es seine Daten mit dem des Servers ab und lädt bei Änderungen das neue Material herunter.

Obwohl es nie offiziell geworden ist, verwenden die meisten Seiten und Programme dasselbe Symbol um auf RSS hinzuweisen.

In unserer DiskStation kommt RSS standardmäßig im Blog zum Einsatz.

Die Geschichte von RSS ist nicht ganz einfach. Da der Standard nie lizenziert wurde oder jemand offiziell dessen Entwicklung übernommen hat, existieren verschiedene Versionen. Zunächst gab das Netscape-Netzwerk, welches der Nachrichtenteil des gleichnamigen Browsers ist, im Jahre 1999 einen Standard heraus, welcher auf RDF, eine Alternative zu XML, setzte. Diese „Rich Site Summary“ wurde aber bald durch „RDF-Site-Summary“ im Jahr 2000 abgelöst, welches inoffiziell von UserLand-Software weiterentwickelt worden war und Version 0.91 darstellte. Bald veröffentlichte man auch 0.92 sowie Entwürfe für 0.93 und 0.94. Parallel zu 0.91 wurde von einer unabhängigen Entwicklergruppe die Version 1.0 geschaffen, welche wiederum auf RDF basierte und ebenfalls im Jahr 2000 veröffentlicht wurde. UserLand stellte seine Arbeiten aber nicht ein und entwickelte bis 2002 die Version 2.0 welche wiederum unter Kritik steht, da es nicht vollständig abwärtskompatibel zu 0.9x ist. Doch da es die aktuellste Version darstellt, setzt es sich trotzdem immer weiter durch.

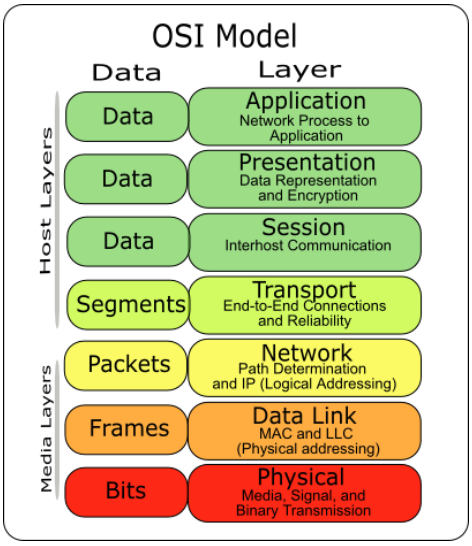
Als Alternative zu RSS-Feeds haben sich Atom-Feeds etabliert, welche ihrerseits auf RSS 2.0 basieren.

1.9 „Layer 8-Probleme“ und eine letzte Übersicht

Wenn Sie mal etwas von einem dubiosen achten Layer hören, sollten Sie Ihre Ohren spitzen. Denn hinter diesem versteckt sich im Internet-Sprachgebrauch meist der Benutzer, also der, der vor dem Bildschirm sitzt.

[22] „Content Managament Systeme“ – automatisierte Webanwendungen welche das Publizieren eigener Webangebote mittels graphischer Oberflächen erleichtern
[23] Extensible Markup Language – Textdatei mit einer definierten Struktur von Elementen und Inhalten

Und um das Thema nun noch abzurunden, hier eine letzte Übersicht für die offiziellen Layer (Unter GPL-Lizenz von: http://commons.wikimedia.org/wiki/File:Osi-model-jb.png).



1.10 Abkürzungen und Fremdwörter

Da, wie bereits ersichtlich, viele Abkürzungen und Fremdwörter zur Verwendung der DS wichtig sind, habe ich eine Liste dementsprechend erstellt. Sehr gut zum neben die Tastatur legen ☺

Abkürzungen und Fremdwörter für Synology DS (CS, RS)

Abkürzung	Bedeutung – Beschreibung
admin	Administrator – Bezeichnung für den Nutzer eines Rechners oder Netzwerks mit den höchsten Rechten, kann alle Einstellungen uneingeschränkt ändern, für Linux siehe „root“
AppleTalk	Protokoll welches Freigaben in einem Netzwerk von Apple-Computern verwaltet
Backup	Kopie von Daten welche im Falle des Dateiverlusts zum Wiederherstellen herangezogen werden kann
Beta	Software im Beta-Status richtet sich an Programmierer und erfahrene Nutzer welche neue Funktionen testen möchten und eigene Software daran anpassen müssen, nicht für den produktiven Einsatz geeignet
CIFS	Common Internet File System – erweiterte Version von SMB, unterstützt u.a. Druckerfreigabe, erweiterte Dateifreigabe, NT-Domänendienst, Papierkörbe
CLI	Command Line Interface – Bezeichnung für eine Administrationsoberfläche auf Textbasis. Im Gegenteil zu GUI wird hier auch auf eine Maus meist verzichtet. Beispiele sind: Telnet, bash, Windows Power Shell
CPU	Central Processing Unit – dt. Prozessor, Kern eines PC/NAS/… welcher zentrale Bedeutung für die Rechengeschwindigkeit besitzt
DDNS	Dynamic Domain Name System – Spezielle Auslegung von DNS um auch ständig wechselnde IP-Adressen aufnehmen zu können
DHCP	Dynamic Host Configuration Protocol – ermöglicht dynamische Vergebung von IP-Adressen in einem Netzwerk, somit müssen nicht mehr alle IP-Adressen manuell vergeben werden
DLNA	Digital Living Network Alliance – Vereinigung von Unternehmen welche einen einheitlichen UPnP-Standard umsetzen und somit reibungslose Kommunikation zwischen ihren Geräten ermöglichen
DMA	Digitaler Medien Adapter – Gerät zum Abspielen von Mediendateien (Musik, Foto, Video) über ein Netzwerk von einem NAS oder Server
DNS	Domain Name System – Geschaffen um das Erreichen einer Adresse zu vereinfachen, wandelt eine Kette von Zeichen in eine IP-Adresse um
DSM	DiskStation Manager – Web-Oberfläche der DS, erreichbar über http://IP_DER_DS:5000 bzw. https://IP_DER_DS:5001
eMule	Tauschbörsenformat ähnlich Torrent um Dateien mit anderen Nutzern zu teilen
eSATA	external SATA – Spezielle Ausführung des SATA-Protokolls zum Austausch von Daten zwischen einem PC/NAS und einem Speichermedium, an meisten DS vorhanden um externe Festplatten zu verwenden
ext	Extended File System – Dateisystem für Festplatten, wird nativ von Linux genutzt
FAT	File Allocation Table – Älteres Dateisystem von Microsoft, Unterstützt keine Dateien größer als 4 GB
Firmware	„Betriebssystem“ für spezialisierte (*embedded*) Systeme
FTP	File Transfer Protocol – Protokoll zur Übertragung von Daten in Netzwerken, aufgrund guter Sicherheit, hoher Geschwindigkeit sowie einfacher Nutzung häufig insbesondere für Webserver und Übertragungen über größere Distanzen und über das Internet verwendet
GUI	Graphical User Interface – Bezeichnung für eine benutzerfreundliche Oberfläche. Meisten Optionen können sowohl mit Tastatur als auch mit Maus geändert werden. Beispiel: DSM
HDD	Hard Disk Device – englische Bezeichnung für Festplatte, zentrales Speicherorgan in Rechnern
Hibernation	Ruhezustand – Prozess welcher Festplatten nach angegebener Minutenzahl herunterfährt, nicht bei Webservern empfehlenswert

http	Hypertext Transfer Protocol – Übertragung von Zeichen über ein IP-Netzwerk (beispielsweise bei Internetseiten)
https	Hypertext Transfer Protocol secure – verschlüsselte Version von http
IMAP	Protokoll zum Abholen von E-Mails wobei die Nachrichten auf dem Server verbleiben und nur temporär zum Ansehen übertragen werden
IP	Internet Protocol – Grundlegendes Protokoll zur Übertragung von Daten in einem Netzwerk
IP-Adresse	Eindeutige Identifikation eines Rechners in einem Netzwerk anhand einer Zeichenkombination, es darf eine Adresse immer nur einem Gerät zugewiesen sein
ipkg	Itsy Package Management System – Software-Verwaltung welche andere Anwendungen einfach aus dem Internet nachladen und installieren kann, auf der DS nur via SSH/Telnet erreichbar/nutzbar
iSCSI	internet Small Computer System Interface – Umwandlung des internen SCSI-Protokolls zur Verwendung über TCP/IP-Netzwerke, äußerst schnell, ist an den PC angebunden wie ganz normaler Festplattenspeicherplatz nutzbar ohne merkbare Unterschiede
ISP	Internet Service Provider – Anbieter von Zugängen zu IP-Netzwerken, in Deutschland mit Bezug auf das Internet auch Internetprovider genannt
Jumboframe	Überschreibt manuell die Einstellung zur Größe von IP-Paketen in einem Netzwerk über dem Standard-Wert von 1518 Bytes
LAN	Local Area Network – Abgeschlossenes Netzwerk welches Freigaben nutzt sowie Drucker und andere Geräte teilt, häufig über ein Netzwerkgerät an das Internet angeschlossen
Local Master Browser	Windows-Dienst welcher die Freigaben in einem Netzwerk verwaltet, kann auf einer Synology-NAS aktiviert werden (kann Probleme beheben aber auch verursachen)
MySQL	Programm zur komfortableren Abfrage, Bearbeitung und Löschung von Daten in SQL-Datenbanken, als spk-Paket bei Synology erhältlich
NAS	Network Attached Storage – bezeichnet an ein Netzwerk angeschlossenen Speicherplatz, auch Synology-NAS gehören dazu, werden von Firmen u.a. genutzt um Backups zu fertigen und selten genutzte Daten von teuren Servern umzulagern
NAT	Network Address Translation – Protokoll zur Manipulation von IP-Adressen in Datenpaketen um 2 Netzwerke zu verbinden, häufig verwendet in Routern um die „Übersetzung“ von mehreren internen IPs auf eine externe zu bewältigen
NFS	Network File System – Dateiübertragungsprotokoll für Netzwerke, stellt Daten so bereit, als wären die Daten direkt auf dem eigenen PC verfügbar
NTFS	New Technology File System – Neuestes Dateisystem für Festplatten von Microsoft, nicht mit Linux kompatibel, stabiler und schneller als FAT
NTP	Network Time Protocol – Mechanismus um Zeiten mit Servern im Internet zu synchronisieren, wichtig u.a. für Mail Station
PHP	Hypertext Pre-processor – Programmiersprache welche dynamische Daten auf Webservern abfragen kann, wird selber nicht übertragen sondern vorher vom Webserver in html umgewandelt
POP3	Protokoll zum Abholen von E-Mails wobei alle Nachrichten auf den PCs des Nutzers übertragen werden
Port	Ports werden hinter IP-Adressen verwendet um jeder Anwendung ein eigenes „Tor“ zu geben, verhindert dass jede Anwendung eine eigene IP zur Ansteuerung benötigt
PPPoE	Point to Point Protocol over Ethernet – Wird von den meisten ISPs verwendet um ihre Kunden anzubinden, von Routern umgewandelt für LAN, wird in den DS unterstützt um eine Verbindung ohne Modem/Router zu ermöglichen

Raid	Redundant Array of Independent Disks –Redundante Anordnung unabhängiger Festplatten erhöht Datensicherheit und Datenverlust bei Hardwaredefekt, erhöht außerdem Schreib- und Leseraten geringfügig, verschiedene Versionen mit unterschiedlicher Anzahl von Platten und unterschiedlicher Sicherheit verfügbar
root	Wird in Linux/UNIX anstatt des Administrators in Windows verwendet um den höchsten Nutzer zu bezeichnen
rsync	Protokoll um Backups zwischen Netzwerk-NAS/Servern anzufertigen, auf meisten Linux-basierten Maschinen verfügbar
S.M.A.R.T.	Self Monitoring, Analyzing and Reporting Technology – System zur Überwachung einer Festplatte und Vorhersage von möglichen Fehlern anhand bestimmter Kennwerte
SMB	Server Message Block – Netzwerkprotokoll zur Übertragung von Dateien und anderen Freigaben, Standardverbindung für Netzlaufwerke unter Windows
SMTP	Simple Mail Transfer Protocol – Protokoll zum Senden und Weiterleiten von E-Mails
SNMP	Simple Network Management Protocol – Protokoll welches Daten aufbereitet, zusammenfasst, und über das Netzwerk verbreitet, welche für den Betrieb eines Netzwerkgerätes wichtig sind - wird u.a. für NAS, Server, Switches und PCs verwendet um frühzeitig Ausfälle zu erkennen
spk-Paket	Synology Paketmanagement – wird auf den DiskStation verwendet um Programme via DSM zu installieren und zu nutzen
SQL	Structured Query Language – Datenbanksprache zur einheitlichen Abfrage und Änderung von Inhalten in Datenbanken, in DS in Web Station integriert
SSH	Secure Shell – Verschlüsselte Alternative zu Telnet
SSL / TLS	Secure Sockets Layer / Transport Layer Security – Am häufigsten verwendete Verschlüsslungen für Datenübertragungen auf niedrigster, systemnaher Ebene
Telnet	Dient der Fernsteuerung von Linux/UNIX-Maschinen über ein Netzwerk in Form einer Eingabeaufforderung ohne grafische Oberfläche (CLI)
Torrent	Tauschbörsenformat um Dateien mit anderen Nutzern zu Teilen über ein verteiltes Netzwerk
Transkoder	Umwandeln einer Mediendatei in ein anderes Format, in der DS verwendet um Dateien vor der Übertragung an einen DMA in ein anderes Format zu verwandeln
UPnP	Universal Plug and Play – Vielseitiges Protokoll um Daten über ein IP-Netzwerk zu übertragen (LAN, Bluetooth, WLAN, FireWire, USB, …)
URL	Uniform Resource Locator – Pfadangabe zu einer Resource in einem Netzwerk über ein geeignetes Protokoll, umgangssprachlich häufig als Synonym für „Internetadresse“ verwendet
USB	Universal Serial Bus – Schnittstelle zwischen einem PC/NAS und einem externen Peripheriegerät, an den meisten DS vorhanden um Festplatten, Drucker etc. anzuschließen
USV	Unterbrechungsfreie Stromversorgung – externe Batterie welche Schwächen und Ausfälle in einem Stromnetz ausgleichen kann und somit ein sicheres herunterfahren von Geräten ohne Datenverlust ermöglicht
Volume	Partition – Unterteilt den Speicher auf einer Festplatte in unterschiedliche Sektionen und formatiert sie
VPN	Virtual Private Network – Prozess der Einbindung eines Laptops oder anderen PCs in ein LAN via Internet
WAN	Wide Area Network – Zusammenschluss mehrerer LAN-Verbindungen um Freigaben und andere Dienste gemeinsam zu nutzen
Webmail	Web-Oberfläche zur Administration eines E-Mail-Postfaches
Workgroup / Arbeitsgruppe	Unterteilt ein Netzwerk in eine oder mehrere Arbeitsgruppen unter Windows, ermöglicht das Teilen von Dateien, Mediendateien, Druckern und anderem

Eine stets aktuelle Liste gibt es hier:

http://matthieu-ds.dyndns.org/abk

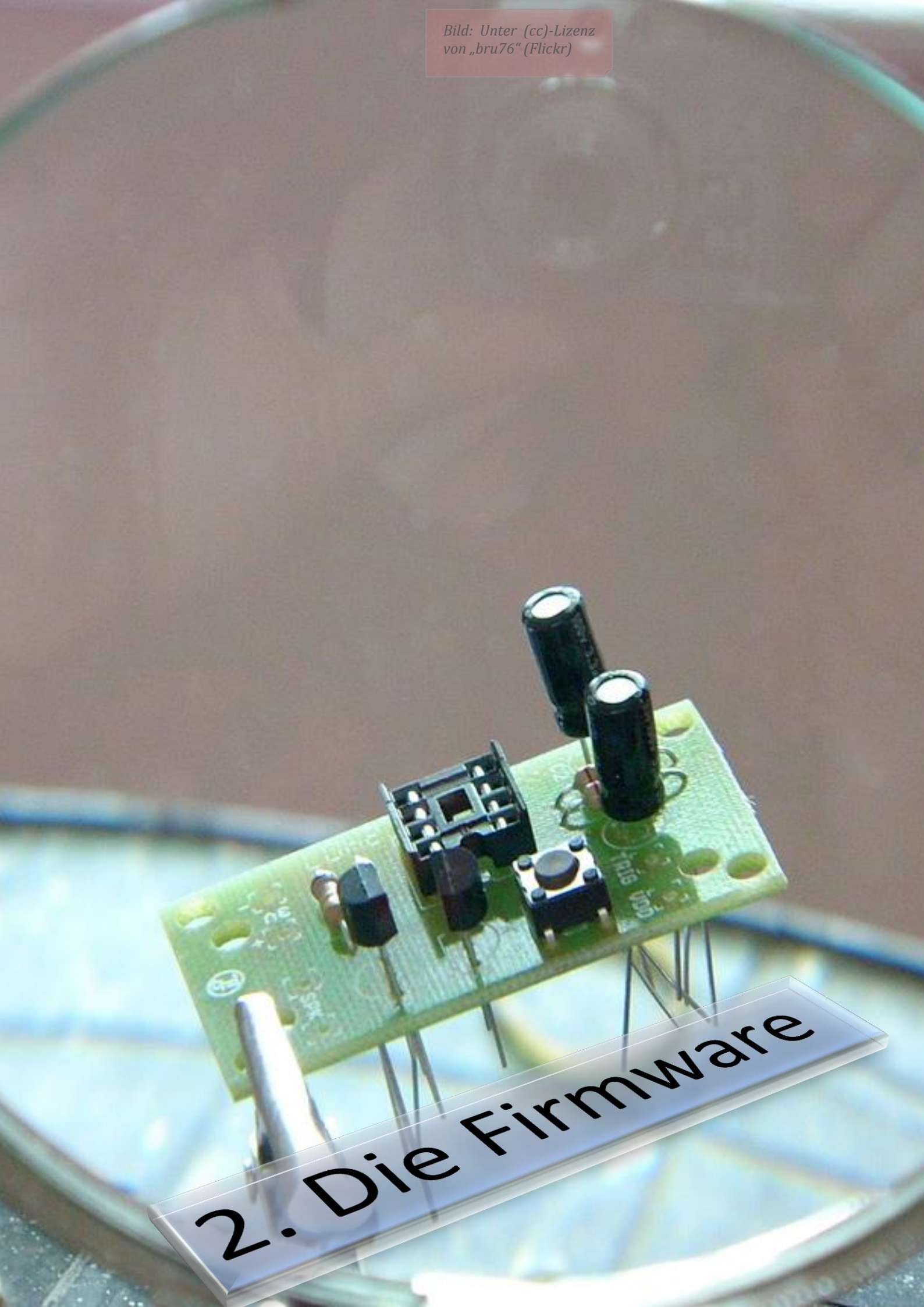


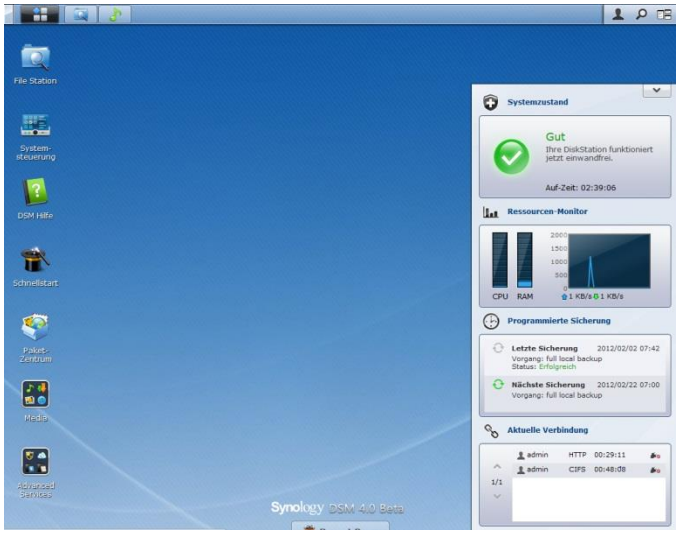
Bild: Unter (cc)-Lizenz von „bru76“ (Flickr)
2. Die Firmware

2 Die Firmware: Vom schlanken Desktop und vielen Paketen

Achtung: Neben Standardfunktionalitäten des DSM sind zwischen den Beschreibungen auch System-Änderungen, sogenannte Modifikationen oder „Mods" eingefügt, welche von Synology nicht unterstützt werden. Auch wenn ich so sorgfältig wie mir möglich arbeite, kann es immer wieder passieren dass entsprechende Hinweise fehlen. Eventuelle Fehler bitte ich daher zu entschuldigen und bei Änderungen am System möchte ich ausdrücklich darauf hinweisen: Alles erfolgt ausdrücklich auf eigene Gefahr!

2.1 Desktop

Der mit DSM 3.0 eingezogene Desktop wird von Synology immer weiter entwickelt. Was auf den ersten Blick vielleicht etwas verspielt wirkt, versteckt viele Funktionen und ermöglicht so eine sehr schnelle Administration und ein sehr flüssiges Arbeiten im Alltag – vorausgesetzt man weiß wo sich die wichtigsten Funktionen befinden. Doch der sehr Desktop-nahe Ansatz sollte den Einstieg sehr erleichtern. Dieses Kapitel behandelt daher die Weboberfläche mit den darauf befindlichen Anwendungen. Genaueres zum Netzwerkzugriff auf eine Disk Station mit anderen PCs gibt es in Kapitel 5.



Sofort erkennbar sind die Taskleiste am oberen Rand mit allen geöffneten sowie den „festgepinnten" Programmen, das Menü über die Schaltfläche links oben, die Desktop-Verknüpfungen und die kleinen Symbole rechts oben die wohl am ehesten mit dem „Systray" vergleichbar sind, also dem Bereich wo bei herkömmlichen Desktops laufende Dienste ein Icon hinterlassen können. Etwas individuell für diesen Desktop sind die Widgets auf der rechten Seite. Dort ist der Systemstatus schnell einsehbar und auch aktuelle Verbindungen, Log-Nachrichten und einiges mehr lassen sich auf einen Blick nach dem Anmelden ablesen. Die (je nach Fenstergröße) bis zu vier Felder lassen sich mit verschiedenen Widgets belegen.

Noch kurz ein Wort zu den Icons rechts oben: Die Grafik eines Oberkörpers führt zu den persönlichen Optionen des Benutzers (Desktop, Speichervolumen, Passwort, u.a.) und dem Abmelden-Knopf. **Über die Suche (Lupen-Grafik) kann nach Anwendungen sowie in der Hilfe gesucht werden. Eine Dateisuche ist hier nicht möglich!** Die letzte Schaltfläche stellt alle geöffneten Anwendungen nebeneinander dar, wie gerade Mac-Nutzer es gewohnt sein dürften.

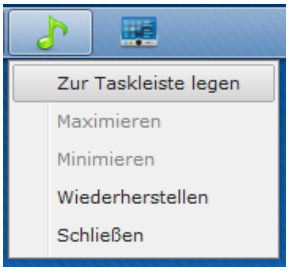
Neue Benutzer sollte man auf diese drei Icons aufmerksam machen, da gerade der „Abmelden"-Button sonst nicht sofort zu finden ist und auch die Einstellungen aus Windows-Manier heraus wohl eher im Menü gesucht werden dürften.

Administratoren hingegen dürfte etwas anderes wichtig sein: Woher kommen die verschiedenen Anwendungen auf dem Desktop und wie vergibt man entsprechende Berechtigungen.

Keine Angst, eines nach dem anderen.

2.1.1 Individualisieren der Oberfläche

Auch wenn man auf diesem Desktop wohl nicht täglich mehrere Stunden arbeitet, ist es doch angenehm einen persönlichen Touch hinzuzugeben oder auch einfach nur persönliche Arbeitsabläufe zu beschleunigen.



Zu letzterem dürften wohl insbesondere die Shortcut-Ordner und die auf die Taskleiste „gelegten“ Anwendungen zählen. Einen Ordner auf dem Desktop erstellt man, indem man ein Symbol nimmt und es auf ein anderes zieht. Über das grüne „+“-Symbol wird signalisiert dass ein Ordner mit diesen beiden erstellt wird. Anschließend lässt sich der Name verändern. Anwendungen die man noch häufiger benötigt lassen sich in der Taskleiste am oberen Bildschirmrand fest „anlegen“ (Anwendung öffnen und mit einem Rechtsklick auf das Symbol in der Taskleiste das Menü öffnen). Auf dem Screenshot sind dieses Menü sowie ein „angelegtes“, jedoch nicht aktives Symbol zu erkennen.

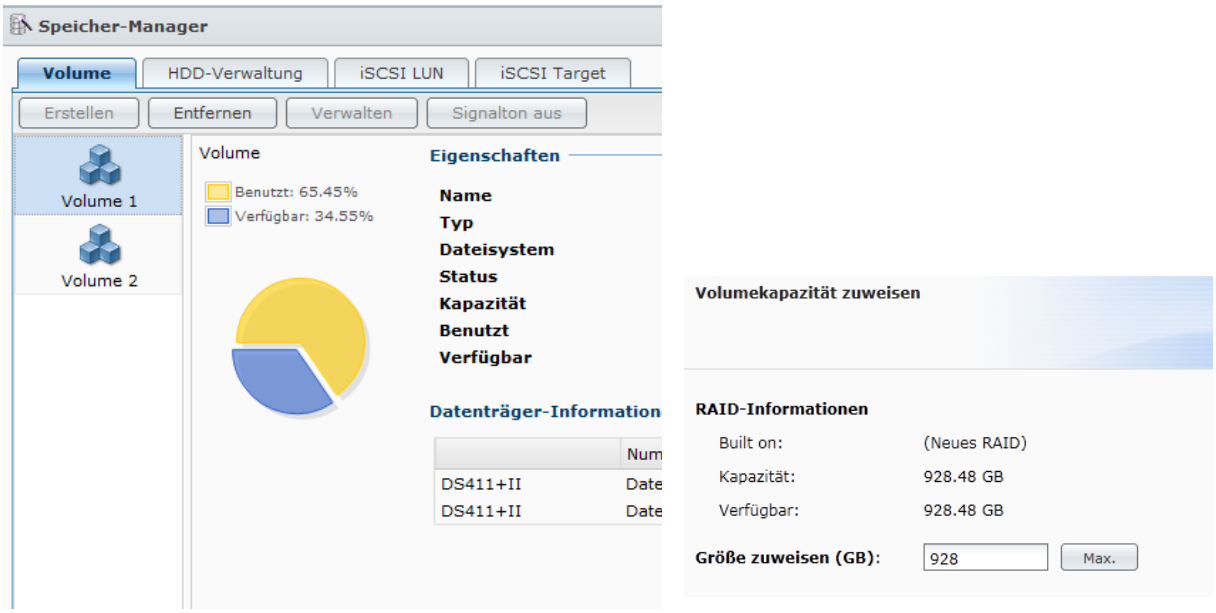
Der Bildschirmhintergrund ist dagegen recht unspektakulär veränderbar: Auf die Person im Tray rechts oben klicken, „Optionen“ und dann „Desktop“ wählen.

2.2 Speicher-Manager

Desktop schön und gut, aber speichern kann man auf einer DiskStation erst einmal noch nichts. Der erste Weg führt über den Speicher-Manager. Denn standardmäßig sieht die Aufteilung der Festplatten wie folgt aus:

- Systempartition welche als großes Raid-1 auf alle Festplatten gespiegelt wird und die Firmware enthält
- Swap-Partition, eine Art Erweiterung des Arbeitsspeichers, bei Linux-Systemen üblich
- Viel leerer Platz welcher durch den Speicher-Manager zugewiesen werden kann – im DSM Volumen genannt und mit „volumeX“ durchnummeriert, beginnend mit „volume1“

Ein Volumen ist dabei ungefähr mit einer Partition vergleichbar, mit der Einschränkung auf nur ein Volumen pro Festplatte. Dazu muss „Basis“ gewählt werden. „Standard“ ist für den Speicher-Manager das Synology Hybrid Raid (SHR), welches den nutzbaren Festplattenplatz optimiert indem es mehrere Raids anlegt. Es hebt damit die Einschränkung eines klassischen Raids auf gleiche Plattengrößen auf. Dennoch besteht stets eine Redundanz von einer Festplatte. Das heißt, eine Festplatte kann stets ausfallen ohne den laufenden Betrieb zu beeinträchtigen. Auch lässt sich ein komplettes Volumen hier als iSCSI-Target zur Verfügung stellen. Doch auch wer ein einfaches, kleines iSCSI-Volumen wünscht, muss über den Volumen Manager gehen. Für die Beschreibung der weiteren möglichen Raids lohnt ein Blick in 1.1.1.



Es ist auch möglich, verschiedene Volumen auf einer Festplatte zu verwenden. Dazu muss man sich jedoch tief in die „benutzerdefinierten“ Einstellungen beim Erstellen des Volumens vordringen. Die Veränderung der Größe ist ebenfalls nachträglich möglich, wenn die entsprechende Festplatte groß genug ist.

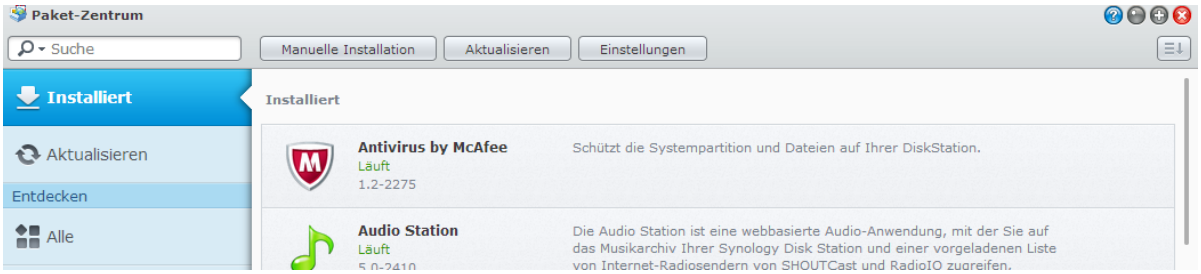
2.3 Die Anwendungen

Mit dem DSM 4.0 hat Synology den DSM außerdem radikal abgespeckt. Beinahe sämtliche Anwendungen sind aus der Firmware heraus in eigene Pakete gewandert. Das Kernsystem umfasst im groben Datenspeicherung und -Verteilung, Backup und Sicherheitsfunktionen sowie den E-Mail-Server (ohne Weboberfläche). Alles andere installiert man über das Paketzentrum nach. Dort finden sich dann auch die bereits bekannten Anwendungen Photo Station, Audio Station, Download Station und Medienserver (und natürlich noch einige andere).

2.3.1 Paketzentrum

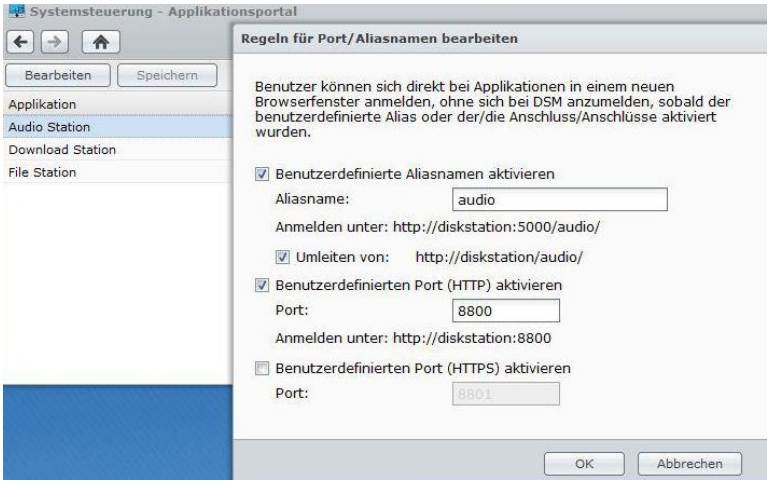
Um Anwendungen zu installieren gibt es das bereits erwähnte „Paketzentrum“. Synology unterteilt dort die selbst aktuell gehaltenen von Anwendungen, welche Fremdentwickler in Kooperation mit Synology verteilen. Dazu gehören u.a. die Groupware Zarafa. Wer hingegen vollständig von Synology unabhängige Pakete sucht, kann die bisher nachinstallierbaren SPK-Dateien gesammelt über Paketquellen beziehen. Diese Quellen bestehen aus einer URL welche in die Konfiguration des Paketzentrums eingefügt werden. Gemeinsam mit QTip hat der Autor dieses Handbuchs den „Community Package Hub“ ins Leben gerufen. Dort kann jeder Entwickler eigene Applikationen hochladen. Das CPH-Projekt ist erreichbar unter „http://www.cphub.de“. Eine Liste mit weiteren Paketquellen befindet sich im Wiki.[24]

[24] Siehe: www.synology-wiki.de/index.php/Paketzentrum_Quellen, abgerufen am 3.3.2013, 17.56 Uhr



2.3.2 Applikationsportal

Wer die einzelnen Anwendungen gerne getrennt laufen lassen möchte und für den Fernzugriff verschiedene Ports vergibt, greift auf das Applikationsportal zurück. Im Groben kann jede Anwendung einen eigenen Port sowie einen Pfad auf dem Webserver bekommen. Letzteres führt dazu, dass etwa bei Aufruf von http://diskstation-ddns/audio (sofern entsprechend konfiguriert) die Audio Station gestartet wird, obwohl man zunächst einen Ordner auf dem Webserver für zuständig befinden würde.

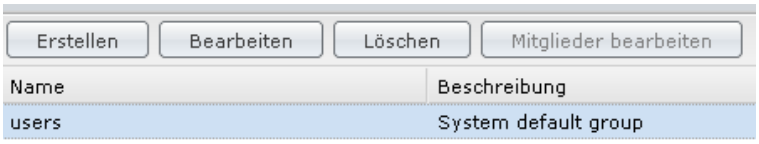


2.4 Berechtigungen – Wer darf was?

Da die genauen Details der Berechtigungen für jeden Nutzer recht kompliziert sind, möchte ich auch darauf noch einmal eingehen. Häufig kommt es im Forum vor, dass Fragen zu den genauen Details dieser Berechtigung gestellt werden. Daher lohnt sich ein guter Blick auf diesen Abschnitt um Probleme zu vermeiden.

Der Punkt im DSM dazu nennt sich „Berechtigungen“. Wenn man von Beginn an eine neue Nutzer-Struktur aufbaut, wovon ich hier einmal ausgehe, ist es sinnvoller mit den Gruppen zu Beginnen.

Im DSM sieht das dann so aus:



Unter „Erstellen“ kann man eine neue Gruppe erstellen. Als Beispiel eine Gruppe namens „Lokal“, welche nur im internen Netz genutzt werden soll und nicht von extern. Dementsprechend wäre eine Freigabe des Ordners „web“ z.B. nicht angebracht. Die anderen Optionen sprechen denke ich für sich.

Nun ist hier aber auch schon die erste schwierigere Stelle: Wenn ein Nutzer mehreren Gruppen angehört, kommt es folglich zu Konflikten. Daher gibt der DSM dem Nutzer immer **so wenig Rechte wie nötig**. Wenn also ein Nutzer in der Gruppe „Lokal“ keinen Zugriff auf „web“ bekommt, dafür aber

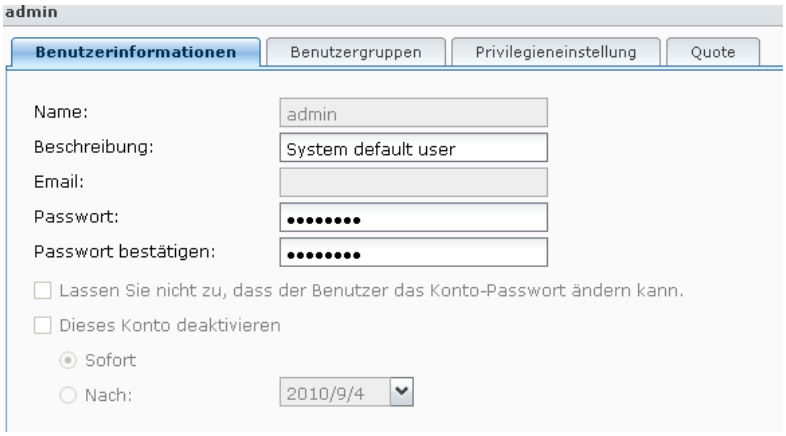
in einer anderen Gruppe sogar mit Schreibrechten ausgestattet wurde, wird er dennoch nicht auf „web“ zugreifen können.

Wenn mehrere Nutzer Zugriff auf die administrativen Funktionen wie „Systemsteuerung“ bekommen sollen, so müssen sie Teil der Gruppe „administrators“ sein. Seien Sie daher vorsichtig, wem Sie zum Administrator machen!

Als nächstes geht es darum, einzelne Nutzer zu erstellen. Das entsprechende Interface sieht so aus:

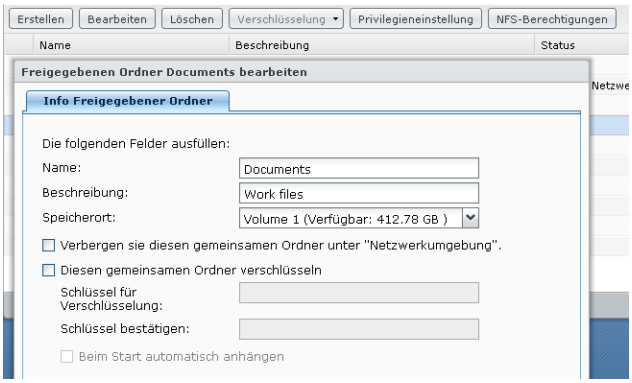
Über den Button „Benutzer importieren“ können Dateien hochgeladen werden, welche detaillierte Informationen zu den einzelnen Nutzern erhalten. Genaueres dazu finden Sie in der Hilfe, welche in den DSM integriert ist. Über „Benutzer-Home“ lässt sich der „home“-Ordner aktivieren und konfigurieren.

Unter „Bearbeiten“ findet sich das folgende Fenster:
(Beispiel für Nutzer admin)



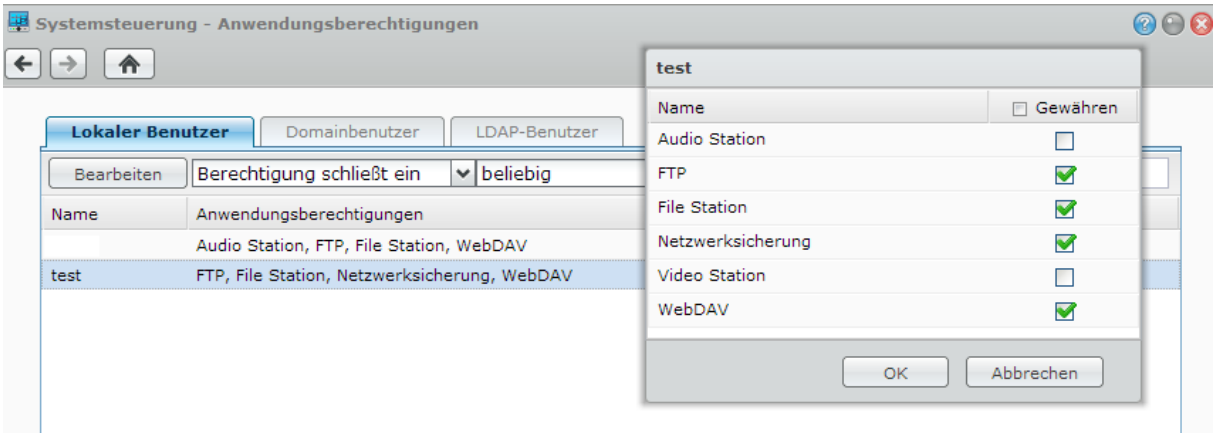
Den Namen sollte man besser nicht ohne weiteres ändern. Die Beschreibung ist nur für eine bessere Übersicht und spielt keine wichtige Rolle. Dasselbe gilt für das E-Mail-Feld. Wahlweise können auch einzelne Nutzer, wie beispielsweise die „Gast“-Accounts deaktiviert werden. Über die anderen Tabs kann die Zugehörigkeit zu Gruppen, die genauen Berechtigungen für die gemeinsamen Ordner und ein optionales Speicher-Limit eingestellt werden, um den Platz für diesen Nutzer zu limitieren.

Die Seite „Gemeinsame Ordner“ bietet eine weitere Möglichkeit, die Zugangsberechtigungen für jeden Nutzer über eine simple Oberfläche zu ändern. Jedoch ist dies nicht unbedingt nötig, da selbige Aufgabe auch an vielen anderen Stellen gelöst werden kann und außerdem die Gruppen-Einstellungen die Rechte gesetzt haben sollten:



2.4.1 Berechtigungen zu Anwendungen

Zu guter Letzt noch einen Blick auf die „Anwendungsberechtigungen“:



Dort kann über einfache Haken die Berechtigung für den Zugang zu den verschiedenen Anwendungen wie FTP, File Station etc. gesetzt werden. Welche Anwendungen auf dieser Seite auftauchen hängt natürlich zum einen davon ab, welche Anwendungen installiert sind, zum anderen muss aber auch der Entwickler seinerseits entsprechende Vorkehrungen treffen. Wer viele der Anwendungen für sich nutzt, wird diese Seite schnell zu schätzen lernen.

2.5 Web Station

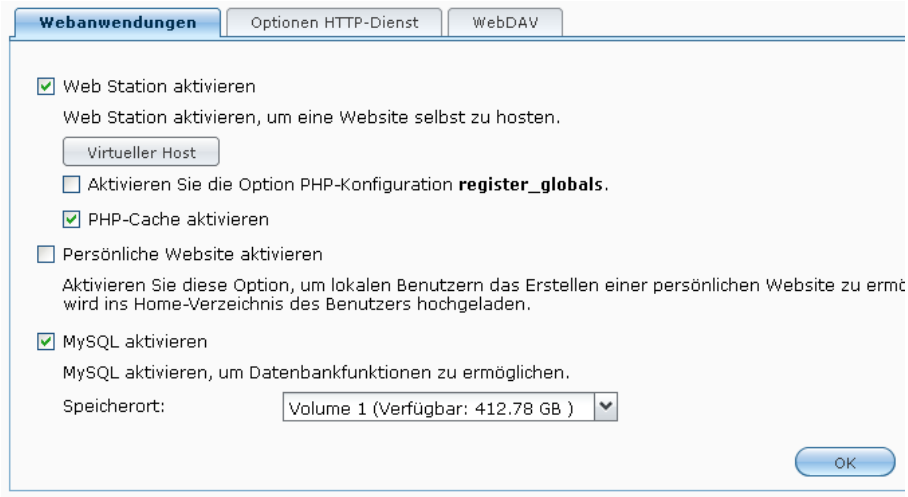
Die Disk Station bringt auch einen eigenen Webserver mit, welcher nach Aktivierung die eigene Homepage im Internet präsentiert. Doch alles der Reihe nach. Zunächst sollten sie sich vergewissern, dass die Web Station im DSM aktiviert ist und die entsprechenden Ports in ihrem Router weitergeleitet wurden (http: 80). Wer das verschlüsselte https nutzen möchte, muss auch dies vorher aktivieren. Nun erstellt die Firmware den Ordner „web“. Dorthin geladene Seiten sind ab sofort über die Adresse der Disk Station erreichbar (http://DiskStation/). Zu beachten ist nur, dass der Webserver nach einer Datei namens „index.html“ (oder „index.php“) sucht und diese zuerst öffnet. Existiert eine solche Seite nicht, erhält der Besucher nur eine Fehlermeldung. Bevor Sie sich jetzt aber auf die Vielzahl der verfügbaren Programmiersprachen stürzen, müssen wir auch auf diese noch einmal kurz eingehen.

Bei den Web-Programmiersprachen wird grundsätzlich zwischen zwei Techniken unterschieden. Die erste Kategorie sind die clientseitigen Programmiersprachen. Wenn ein Nutzer auf eine Seite zugreift, welche clientseitige Programmiersprachen nutzt, wird der Klartext übertragen und dann im Browser des Nutzers in etwas Visuelles umgesetzt. Die wohl am häufigsten genutzten, clientseitigen Sprachen sind JavaScript (DOM), ActiveX, Flash und html. Diese Sprachen können Sie ungehindert einsetzen, da

sie keine Anforderungen an den Webserver stellen. Bei Betrachtung der serverseitigen Sprachen ist hingegen etwas Vorsicht geboten. Denn hier muss der Webserver, in diesem Fall ein Apache (eventuell einigen vom XAMPP-Paket bekannt), den Code umsetzen und dann in html-Form an den Client schicken. Die Disk Station unterstützt ausschließlich PHP und (nach Aktivierung) auch eine entsprechende Anbindung an MySQL. Dies sollte für die meisten Heimprojekte eigentlich genug sein. Doch der Vollständigkeit halber seien mit JSP, ASP und Perl auch nicht unterstützte Techniken genannt.

Um nun den Zugriff auf die neue Webpräsenz zu erleichtern, sollte man sich darüber hinaus einmal DDNS ansehen.

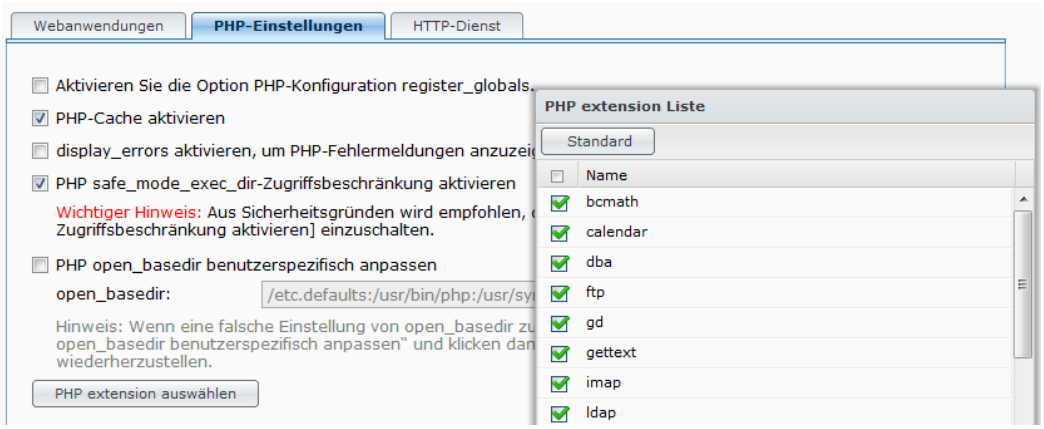
Unter der Haube kommt bei Synology wie schon angesprochen ein Apache-Webserver zum Einsatz welcher die meisten häufig genutzten PHP-Module beinhaltet. Doch an vielen Ecken wurde auch gespart um die Geschwindigkeit zu erhöhen. Wer also die volle Kontrolle haben möchte, der kann sich einen zusätzlichen Apache via ipkg installieren und diesen entsprechend anpassen und erweitern. Entsprechende Anleitungen gibt es im deutschen Synology-Forum und Wiki.[25]



2.5.1 Erweiterte PHP-Einstellungen

Der Webserver ist mittlerweile zu einem wichtigen Bestandteil der Firmware geworden der von vielen genutzt wird. Daher ist es auch wichtig, entsprechende Konfigurationsmöglichkeiten zu bieten. Die weitreichendsten Optionen sind in Bezug auf PHP vorzufinden.

[25] http://www.synology-forum.de/showthread.html?t=1852, http://www.synology-wiki.de/index.php/Apache_IPKG



Die Funktion „register_globals“ ist seit Version 4.2 von PHP (veröffentlicht 2002) standardmäßig deaktiviert. Zu groß waren die Sicherheitslücken welche entstanden. Über diese Funktion konnten externe Skripte und Dateien einfach Daten in ein laufendes PHP-Programm schreiben, was Tor und Tür für eine Vielzahl an Schädlingen öffnete, die ein einfaches Skript damit zweckentfremden konnten.

Der PHP-Cache ist da schon deutlich nützlicher. Wenn der Webserver sehr stark frequentiert wird, muss dennoch jedes Skript bei jedem Aufruf neu bearbeitet werden. Auch wenn dabei häufig dasselbe herauskommt, etwa bei einer Navigation für eine Webseite welche aus einer Datenbank stammt. Ein Cache speichert solche Ergebnisse insbesondere aus Datenbanken zwischen und verwendet sie eine Zeit lang wieder. Wenn man hingegen gerade eine neue Webseite entwickelt, kann das durchaus stören.

Um den Nutzer nicht mit banalen Warnhinweisen durch PHP zu verunsichern weil der Entwickler hier oder da ein wenig unsauber gearbeitet hat, werden einige Meldungen von PHP nicht angezeigt. Entwickelt man hingegen eine neue Seite, sind solche Informationen manchmal wichtig, weil sie zeigen wo etwas nicht das macht was es soll. Genau dafür ist „display_errors“ angelegt.

Hinter dem etwas umständlichen „safe_mode_exec_dir“ steckt eine PHP-Funktion um Befehle auf der Systemebene auszuführen. Da PHP somit aber weitreichende Möglichkeiten bekommt das lokale System zu verändern, kann bei einem Sicherheitsleck die Disk Station mit Schadsoftware versehen oder umkonfiguriert werden. Standardmäßig beschränkt der Webserver die Funktionalität daher.

„open_basedir“ legt fest, auf welche Verzeichnisse der Webserver Zugriff hat. Insbesondere die Web Station hat nur sehr eingeschränkte Zugriffsrechte auf die Daten. Hier lässt sich einsehen und ändern, auf welche Daten konkret zugegriffen werden kann. Doch Vorsicht: Eine falsche Option und ihre gesamten Dokumente sind möglicherweise online ohne Zugangsdaten abrufbar!

Die PHP Extensions sind vergleichbar mit Plugins oder Add-Ons wie es sie für viele Anwendungen gibt. PHP lernt damit beispielsweise Verschlüsselung, Archive entpacken, mit Datenbanken umgehen und noch einiges mehr. Die bereits aktivierten sollte man belassen, da sie häufig für CMS-Systeme und andere „Fertigprodukte“ notwendig sind. Wünscht man sich mehr Funktionen oder wird man bei der Installation eines CMS nach einer anderen Extension gefragt, lohnt ein Blick in die Liste durchaus.

2.5.2 Zugriffschutz eigener Seiten mit .htaccess

Was aber, wenn man nun einzelne Seiten der Allgemeinheit vorenthalten möchte und daher per Passwort versucht abzusichern? Der einfachste Weg führt bei unserem Apache über eine .htaccess-Datei. Genau genommen müssen wir zwei Dateien erstellen: Zum einen die .htaccess und eine

weitere, welche Nutzernamen und Passwörter enthält. Der Einfachheit halber, gehen wir davon aus, dass wir alle Seiten schützen möchten. Daher erstellen wir zunächst als Ablage für unsere Dateien einen Ordner „passwd“ im Stammordner „web“ des Apache. Nun erstellen wir mit einem einfachen Editor eine Datei mit folgendem Inhalt:

```
AuthName "Title"
AuthType "Basic"
AuthUserFile "/volume1/web/passwd/nutzer.pw"
require valid-user
```

Jetzt nennen wir diese Datei „.htaccess“ (Punkt nicht vergessen!). Wie wir sehen, wird im Code auf die Datei „nutzer.pw“ verwiesen. Dies ist die Datei, welche später die Zugangsdaten enthält. Also erstellen wir eine Datei nach folgendem Schema:

```
Nutzer:Passwort
```

Außerdem dürfen wir pro Zeile immer nur einen Nutzer einfügen. Da dieses System aber verhältnismäßig einfach zu knacken wäre, wird das Passwort stets verschlüsselt. Dazu gibt es im Internet eine ganze Reihe von .htaccess-Generatoren. Nun könnte unsere Datei zum Beispiel so aussehen:

```
Admin:$1$3a6ec4Pk$YiEMOVnuxlzRkQoEmLaPS0
Heinz:$1$vOb0WUyG$MnoANxLYwI2JWOSc96At5
```

Nun laden wir noch die Datei .htaccess in das Verzeichnis“ /web“ und die nutzer.pw in das Verzeichnis „/web/passwd“. Wer allerdings nur Unterverzeichnisse sperren möchte, legt die .htaccess dort hinein.

Um die Sicherheit noch weiter zu erhöhen, kann man die nutzer.pw auch in ein anderes Verzeichnis als „web“ legen und erhöht somit noch einmal die Sicherheit, da somit kein direkter Zugriff auf die Datei vom Web aus mehr möglich ist.

Dieses kleine Beispiel schöpft bei weitem nicht die Möglichkeiten der .htaccess aus. Mehr Informationen findet man zu Hauf im Internet.

> ***Weiterführende Informationen zum Thema .htaccess finden Sie auch im eigens dafür erstellten Kapitel 9.***

2.5.3 Suchmaschinen abweisen

Suchmaschinen wie Google und Yahoo erleichtern uns das Leben im Internet jeden Tag enorm. Doch private Seiten sollten nicht unbedingt überall katalogisiert sein. Dafür gibt es „robots.txt“-Dateien. Die meisten Suchmaschinen prüfen erst nach dieser Datei bevor sie mit ihrer Arbeit beginnen. Einfach eine Datei „robots.txt“ mit folgendem Inhalt in das Verzeichnis „/web“ hochladen:

```
User-agent: *
Disallow: /
```

Was genau passiert hier? Zunächst wird definiert für welchen Browser diese Einschränkungen gelten. Da die robots.txt nur von Suchmaschinen genutzt wird, kann man hier einfach alle Browser-Typen auswählen. Um eine optimale Darstellung zu erreichen, sendet jeder Browser beim Aufruf der

Seite eine kurze Anmerkung mit seinem Namen und Version. Schließlich wird die Datei noch für das gesamte Verzeichnis („/“) aktiviert.

2.5.4 Alle Zugriffe auf den Webserver loggen

Wer möchte nicht gerne mitlesen, wer die eigene Seite besichtigt. Mit einer kleinen Änderung im Apachen zeichnet er alle IP-Adressen auf. Dafür müssen wir uns per SSH/Telnet auf unseren Server als „root“ einloggen. Oder man hat bereits einen Editor als Anwendung via spk installiert (siehe Kapitel 15.3.2). Als nächstes sichern wir die Datei, welche wir gleich bearbeiten werden:

```
cd /usr/syno/apache/conf
cp httpd.conf-user httpd.conf-user-backup
```

Nun öffnen wir unsere Datei:

```
vi httpd.conf-user
```

… und suchen den Eintrag „CustomLog /dev/null combined“ (normalerweise irgendwo zwischen Zeile 200 und 220). Jetzt muss er noch ersetzt werden:

```
CustomLog /volume1/web/log/access.log combined
```

Zwar werden jetzt alle IPs in der Datei „access.log” gespeichert, doch da das Verzeichnis „/web/log“ noch nicht existiert, würde ein Fehler auftreten. Daher wechseln wir nun das Verzeichnis:

```
cd /volume1/web
```

… und erstellen „/log“:

```
mkdir log
```

Zu guter Letzt müssen wir den Apache-Webserver noch neu starten:

```
/usr/syno/etc/rc.d/S97apache-user.sh restart
```

Dennoch gilt auch hier wieder: Datenschutz beachten! Daten dürfen nicht unbegrenzt mitgeschnitten und gespeichert werden, siehe auch Kapitel 10.5.

2.5.5 Eigener “404-Error”

Die Überschrift ist eigentlich etwas irreführend, denn der Begriff „404-Error“ wird bei der DiskStation nicht verwendet. Stattdessen bekommt man eine automatisierte Seite welche besagt, dass die Seite nicht gefunden werden konnte. Dieser Fehler nennt sich allerdings offiziell „HTTP-404-Error“. Wer nun eine eigene Fehlermeldung ausgeben möchte, erstellt zunächst eine html-Seite ganz nach dem eigenen Geschmack. Nun muss man die Datei in „missing.html“ umbenennen und in das Standardverzeichnis des Webservers „/web“ einfügen. Wer jetzt einfach mal eine nicht vorhandene

Seite versucht zu öffnen, sieht seine neue Fehlermeldung. Eine deutlich ausführlichere Alternative stellt htaccess dar, welches auch für jeden Error-Code eigene Seiten aufrufen kann.

2.5.6 Jedem Nutzer ein Zuhause

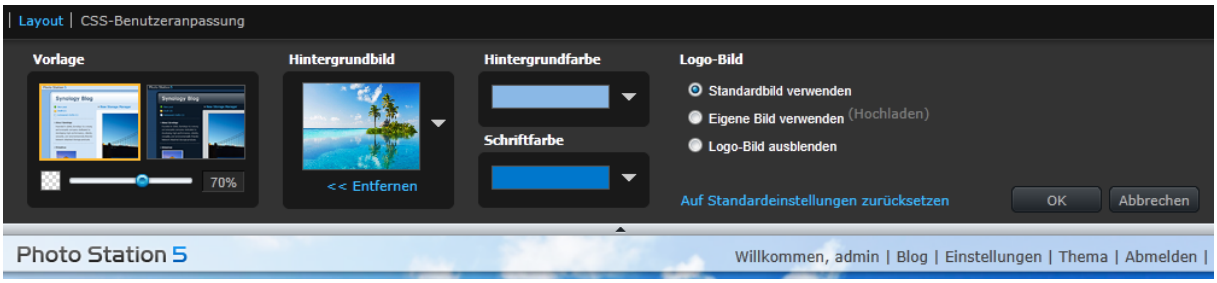
Seit dem DSM 2.1 und der dazugehörigen Firmware 836 gibt es eine neue Funktion, welche jedem Nutzer ermöglicht, einen persönlichen Ordner zu erstellen. Über die Einzelheiten dieser Funktion spreche ich noch später, aber zunächst möchte ich über eine darin integrierte Funktion aufklären, welche jedem Nutzer eine eigene Website ermöglicht. Zunächst muss man diese im DSM einschalten. Idealerweise sollten Sie dies auch ihren Nutzern mitteilen, damit diese entsprechend reagieren können. Als erstes muss der Nutzer im „/home“-Verzeichnis den Ordner „www“ erstellen. Nun ist es auch schon so weit: Die Startseite index.html kann hochgeladen werden. Die Adresse der persönlichen Seite ist wie folgt: http://[DS-Adresse]/~[Nutzer]. Als Beispiel für die DDNS-Adresse „meine-ds.de“ und einen Nutzer namens „Lokal“: http://meine-ds.de/~Lokal.

2.6 Photo Station

Die einzige, von Synology bereits vorinstallierte Webanwendung ist die Photo Station. Diese läuft technisch gesehen auf demselben Webserver wie die Web Station, benötigt diese jedoch nicht unbedingt. Erreichbar ist sie nach Aktivierung über http://diskstation/photo bzw. http://diskstation/~benutzername/photo (Persönliche Photo Station, sofern aktiviert). Auf einer Disk Station gibt es wohl keine bequemere und zugleich vollständigere Lösung zum Veröffentlichen und Präsentieren von Fotos. Dafür kann der Blog mit Hinsicht auf die Features nicht ganz mit großen Systemen wie Wordpress mithalten. Die Auslegung als Webanwendung ohne direkten Bezug zum DSM begründet auch die separate Konfigurationsoberfläche. Um Zugang zu dieser zu erhalten muss man sich mit dem einzigen Benutzerkonto anlegen welches standardmäßig auch hier existiert: Dem admin. Ist man angemeldet, kann man jedoch die Benutzerkonten auch mit denen des DSM koppeln. Die Photo Station greift dann auf Benutzernamen und Passwörter dort zu; nur die Berechtigung auf Basis der Alben muss man weiterhin dort administrieren.

Ein Album ist im Normalfall ein Unterordner von „photo“. Wenn ein Album „öffentlich“ ist, können alle Besucher mit Kenntnis der Domain auch auf die Bilder zugreifen. Darüber hinaus ist neben den üblichen Berechtigungen auch ein reiner Passwortschutz ohne einen echten Account einstellbar. Ebenso lässt sich die Optik sehr gut anpassen, bis hin zum CSS-Code[26]. Zugang zum Editor gibt es über den Button „Thema“ in der Kopfleiste. Die zwei Vorlagen lassen sich durch viele weitere Stellschrauben wie Hintergrundbild und -farbe anpassen.

[26] Eine ganze Reihe von Möglichkeiten ist hier aufgeführt: http://www.synology-wiki.de/index.php/Photo_Station_CSS-Benutzeranpassung, abgerufen am 1.3.2013, 15.20 Uhr



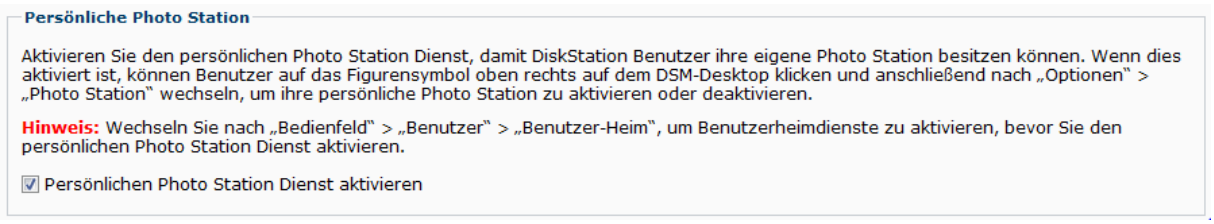
Ab DSM 4.1 ist auch eine Gesichtserkennung in das System eingezogen, sowie eine Zeitleiste auf der nach Kriterien gefilterte Bilder chronologisch und ortsbezogen (sofern Ortsdaten der Bilder vorliegen) aufbereitet werden. Für diese wie auch viele andere Funktionen ist die Software auf sogenannte Meta- oder EXIF-Daten angewiesen. Diese enthalten eine Vielzahl von Eigenschaften zur Datei. Von Kameramodell und Einstellung über Fotograf und Copyright bis hin zu GPS-Ortsdaten. Voraussetzung ist aber, dass entweder die Kamera oder ein Programm zur Nachbearbeitung diese Daten hinterlegen bevor die Datei erstmalig in die Photo Station abgelegt wird.

Die Gesichtserkennung belastet den Prozessor einer Disk Station sehr stark. Außerdem ist das Beschriften der Gesichter über die Photo Station etwas anstrengend. Bei größeren Fotosammlungen kann man daher auch die Windows Live Fotogalerie nutzen. Diese verwendet die Ressourcen des PCs und liefert außerdem bessere Ergebnisse. Nur über WLAN ist die Fotogalerie ziemlich langsam, da die Bilder zur Verarbeitung für kurze Zeit vollständig auf den PC geladen werden. Sie sollten also einen PC mit Ethernet-Kabelverbindung nutzen. Die Geo-Funktion um Bilder mit Ortsangaben zu versehen ist keine Stärke der Fotogalerie. Stattdessen können Sie hier das Programm „GeoSetter“ [27] verwenden, dass allerdings etwas Einarbeitung erfordert.

2.6.1 Persönliche Photo Station

Damit auch die einzelnen Benutzer die Möglichkeit einer eigenen Photo Station erhalten, gibt es die „Persönliche Photo Station“, welche sich in der Photo Station aktivieren lässt. Voraussetzung hierfür sind aktivierte Home-Ordner. Desweiteren muss jeder Benutzer für sich die persönliche Photo Station aktivieren, indem er im Desktop seine Optionen öffnet und dort im Reiter „Photo Station“ diese aktiviert.

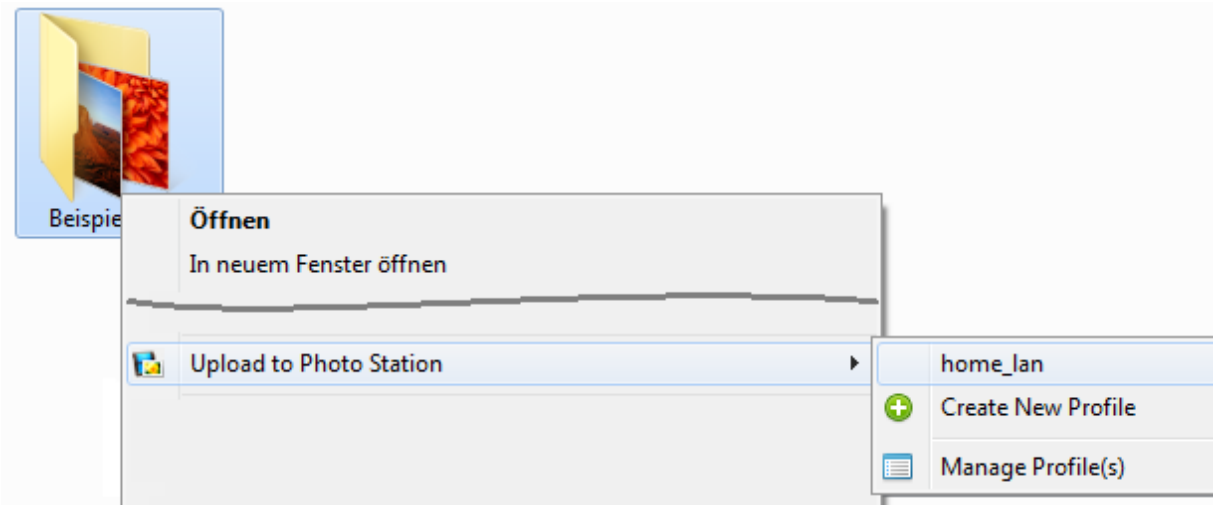
Der admin hat auf diese Photo Station direkt keinen Einfluss! Über „homes“ kann er die dort gespeicherten Bilder ändern – die Rechteverwaltung auf der Photo Station des Benutzers liegt aber außerhalb seiner Reichweite. Die Fotos müssen im Ordner „photo“ unter „home“ liegen. Existiert dieser Ordner nicht, kann man ihn auch selbst anlegen. Der Pfad unter dem die Photo Station erreichbar ist, heißt http://diskstation/~benutzername/photo (wobei „benutzername“ ersetzt werden muss, nicht jedoch das Tildenzeichen!). Es ist also durchaus ratsam, über htaccess einen Alias zu erstellen, denn der lange Pfad ist nicht gerade schön (siehe auch Kapitel 12.2).



[27] Siehe: http://www.geosetter.de/, abgerufen am 24.2.2013, 16.44 Uhr

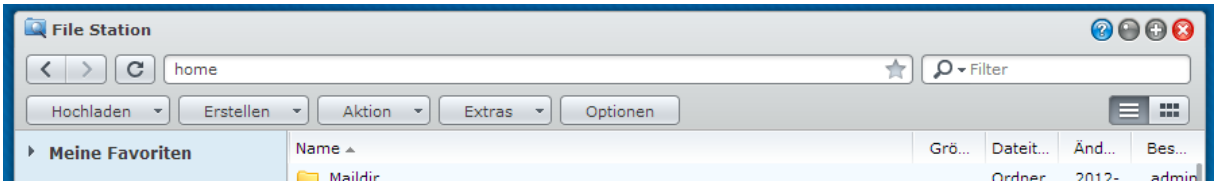
2.6.2 Photo Station Uploader

Das Hochladen von Bildern ist und bleibt ein heikles Thema, denn es wird immer geraume Zeit dauern bis die Vorschaubilder erstellt sind. Und es wird auch immer User geben denen es zu lange dauert. Um das Hochladen über einen PC komfortabler zu machen, hat Synology eine eigene, schlanke Anwendung für Windows geschrieben. Über einen einfachen Rechtsklick können so ganze Ordner der Photo Station hinzugefügt werden. In den verschiedenen Profilen kann zwischen Disk Stations, Benutzern und benutzerdefinierten Photo Stations gewechselt werden, ohne jedes Mal die gesamte Konfiguration neu vornehmen zu müssen. Da die Konfiguration Menügeführt ist und die Anwendung sehr schmal, erspare ich mir an dieser Stelle genauere Erläuterungen. Der Download ist wie immer auf der Synology-Webseite zu finden.



2.7 File Station

Historisch gesehen war die File Station zunächst eine eigene Applikation, die auch separat erreichbar war. Mit der Einführung des Desktop-Ansatzes erfüllt es nun auch die Aufgabe eines „Dateibetrachters“ ähnlich Explorer (Windows) und Finder (Mac). Nutzer einer älteren Version des DSM können allerdings auch auf den „Dateibrowser“ stoßen, welcher eine Zeit lang der Desktop-Ersatz der File Station war. Über die Systemsteuerung des DSM lässt sie sich aber weiterhin als getrennte Applikation einrichten. Vergibt man dort einen eigenen Port, bekommen User den DSM nicht zu Gesicht wenn sie die File Station nutzen sollen. Da die File Station aber über das http-Protokoll läuft, sollte man keine Geschwindigkeitsrekorde erwarten. Gerade im LAN sollte man daher einen Bogen darum machen.

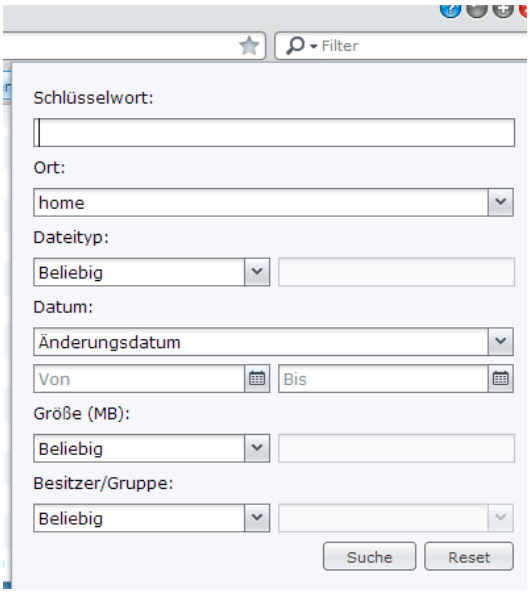


Zu den interessantesten Funktionen gehören:

- Video-Dateien wiedergeben (Rechtsklick auf die Datei, „Wiedergeben“). Dies setzt für viele Dateiarten einen installierten VLC Media Player voraus. Dieser Player ist nach Meinung vieler ohnehin Standardumfang für jeden PC und somit keine „Last“, sondern eher ein Zugewinn

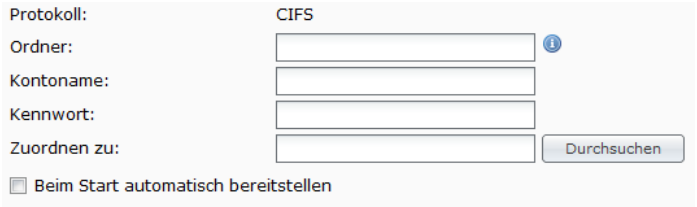
wenn er noch nicht installiert ist. Wichtig ist für Firefox ein aktiviertes „Mozilla-Plugin“ bei der Installation. Nur so ist die Kommunikation Browser-VLC sichergestellt und die Videos funktionieren wirklich.

- PDF’s und Dokumente mit Hilfe von Google Doc’s öffnen (Rechtsklick auf Datei, „In Google docs anzeigen“).
- Fotos auch ohne Photo Station außerhalb des „photo“-Ordners betrachten (Rechtsklick auf Datei, „Vorschau“). Ähnlich funktioniert dies auch mit Videos, setzt aber bei vielen Formaten ein VLC-Plugin für den Browser voraus.
- Bilder über externe Dienste bearbeiten.
- Upload von Dateien über Drag’n’Drop des Windows Explorers (Datei im Explorer nehmen und auf das Fenster des Dateibrowsers ziehen).
- Nach Dateien suchen (Rechts oben im Dateibrowser auf „Erweiterte Suche“ klicken, was ein Menü öffnet). Einen deutlichen Geschwindigkeitsschub ergibt eine Indexierung der Dateien, welche in der Systemsteuerung unter „Gemeinsame Ordner“ aktiviert werden kann.
- … sowie die in den nächsten Unterkapiteln erklärten.

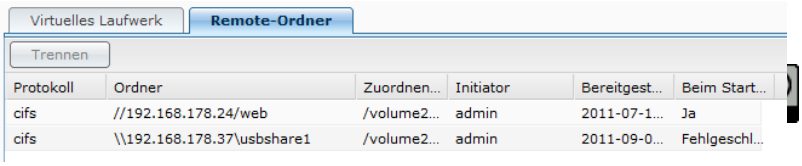


2.7.1 Einhängen von Images (ISO & UDF) und Netzlaufwerken

Weiter vereinfacht wird die Handhabung von größeren Netzwerken mit dem Einhängen von entfernten Verzeichnissen. Die DS bindet („mount“) somit ein Verzeichnis eines beliebigen SMB/CIFS-Servers ein. Wichtig zu beachten ist, dass die Zugangsdaten dabei beim Einhängen angegeben werden – eventuell auf anderen Servern vergebene Berechtigungen greifen somit nicht mehr, da für den entfernten Server alles aussieht als würde es von diesem einen Benutzer kommen.



Ebenso werden Images unterstützt wie sie meist von CDs oder DVDs angefertigt werden. Genau wie Netzwerkordner können diese in ein leeres (!) Verzeichnis eingehangen werden. In diesem Verzeichnis wird somit der Inhalt des Archivs angezeigt. Die Funktionsweise hängt eng mit dem Linux-Betriebssystem zusammen, welches auf diese Art arbeitet und Verzeichnisse so „ineinander“ hängt. Die Anzahl der eingehängten Verzeichnisse ist in beiden Fällen jedoch begrenzt.



Die „Verbindungsliste“ der File Station führt alle eingehängten Verzeichnisse auf.

2.7.2 „home“

Wie bereits beim Webserver angesprochen, gibt es seit dem DSM 2.1 eine Funktion um jedem Benutzer ein persönliches Verzeichnis zu erstellen.

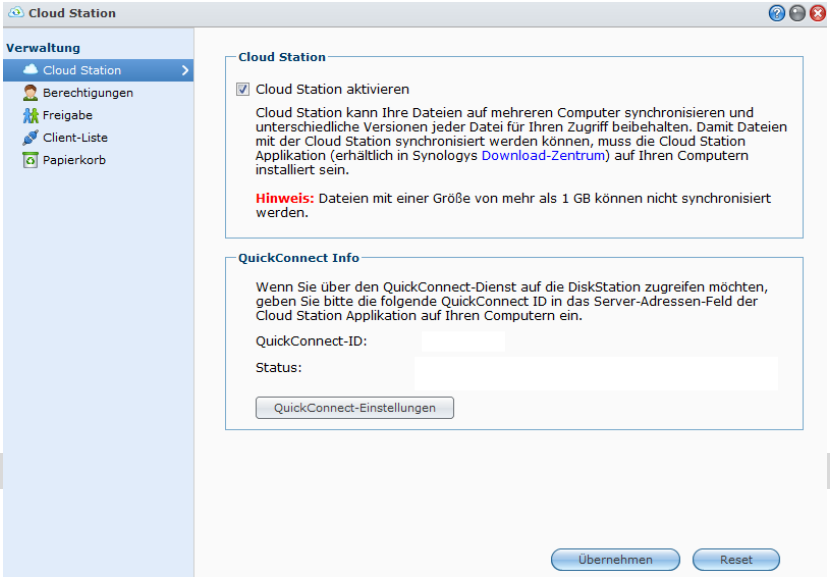
Diese ist vergleichbar mit den „Eigenen Dateien“ eines Windows-PCs. Obwohl für jeden Nutzer sicht- und nutzbar ist der Inhalt an den Nutzer gebunden. Dieser neue Ordner ist fest in die normale Verzeichnis-Struktur eingebunden. Die Zugangsberechtigungen sind fest eingestellt und können nicht via DSM administriert werden. Damit der admin dennoch nicht die Kontrolle über die gelagerten Daten verliert (Thema illegale bzw. unerwünschte Dateien für welche auch der Anbieter teilweise mithaftet), ist für ihn nun zusätzlich zu seinem eigenen home-Ordner ein Ordner „home**s**“ verfügbar. Dort sind Links zu den verschiedenen home-Ordnern jedes einzelnen Nutzers integriert. Es handelt sich dabei allerdings um eine reine Sicherheitsmaßnahme und man sollte es nicht übertreiben.

2.8 Cloud Station

Dienste wie Dropbox sind weithin bekannt und praktizieren seit Jahren was nun gern als „Cloud“ die Runde macht. Bei Synology hat man nun an dies angeknüpft und synchronisiert über verschiedene Geräte hinweg Dateien. Dazu ist das gleichnamige Programm für die DS (nachinstallierbar über das Paketzentrum) sowie das aktuell für Windows und Mac bereitstehende Desktop-Programm notwendig. Anschließend synchronisiert die Cloud das Verzeichnis „CloudStation“ unter dem persönlichen home-Ordner. Eine Änderung des Verzeichnisses ist momentan nicht möglich.

2.8.1 Installieren, aktivieren und richtig nutzen

Über die Cloud Station wird viel diskutiert – vom unglücklichen Name bis hin zum eigentlichen Sinn. Doch wenn man sie richtig benutzt, stellt sie durchaus einen kleinen Ersatz für Dropbox dar. Jedoch sollte man nicht auf die Idee kommen die gesamte Videosammlung zu synchronisieren. Auch bei Dropbox würde man normal nicht auf die Idee kommen, riesige Sammlungen im Terrabyte-Bereich synchron zu halten.



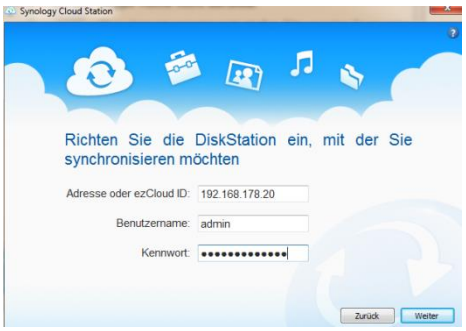
Erster Anlauf ist das Programm „Cloud Station“ auf der Disk Station (bzw. Rack Station). Es lässt sich mit

wenigen Klicks aus dem Paketzentrum installieren. Es lohnt aber durchaus neben der Aktivierung des Dienstes auch die weiteren Konfigurationsmöglichkeiten durchzusehen. Neben der „ezCloud-ID“ werden hier auch Berechtigungen vergeben, verbundene Clients angezeigt und alte Dateien wiederhergestellt. Mit der Aktivierung der Cloud Station hat jeder Benutzer einen eigenen Ordner „CloudStation“ in seinem „home“-Verzeichnis, sofern letzteres aktiviert ist. Möchte man nun zusätzliche Ordner synchronisieren, muss man dies unter „Freigabe“ konfigurieren.

Der häufigste Stolperstein für Probleme mit der Cloud Station sind, neben der soeben angesprochenen „Freigabe“-Liste, die Berechtigungen. Ein neuer Benutzer darf nicht automatisch die Cloud Station verwenden. Er muss dazu unter „Berechtigungen“ freigeschalten werden. Auch über LDAP oder Domänen eingebundene Benutzer betrifft dies.

Als nächstes geht es zurück zum PC/Mac. Die Software kann jederzeit bei Synology heruntergeladen werden und aktualisiert sich bei Updates auch selbstständig über die Synology-Server. Nach der Installation wird man über die Einstellungen ausgefragt. Standardmäßig legt das Programm unter Windows einen eigenen Ordner im Profil des Benutzers an.

Noch eine kleine Anmerkung zur QuickConnect-Funktion: Dieser Dienst läuft über Synology. Verwendet man ihn nicht, laufen auch keine Daten der Cloud Station über Synology (außer die angesprochene Auto-Update-Funktion des Clients). Der Haken daran ist aber auch, dass man nur eine Verbindung zur heimischen Cloud Station herstellen kann, wenn die Synology-Dienste fehlerlos arbeiten. Das war in der Vergangenheit nicht immer so. Man kann aber auch die gleiche Methode anwenden wie mit allen anderen Anwendungen die Fernzugriff verwenden: DDNS und Portfreigabe. Der Port für die Cloud Station ist standardmäßig 6690 und die Kommunikation erfolgt, sofern nicht anders im Client konfiguriert, verschlüsselt.



Öffnet man den zu synchronisierenden Ordner, kann man im Windows Explorer kleine Symbole über den einzelnen Elementen sehen. Auch das Symbol in der Taskleiste klärt über den aktuellen Status auf. Gibt es mehrere Versionen einer Datei von verschiedenen Geräten, so erstellt die Cloud Station im Übrigen eine neue Datei mit anderem Namen. So können Konflikte erkannt und behoben werden. Diese lassen sich gelegentlich nicht vermeiden wenn Benutzer die Dateien auch offline nutzen können.

Die Cloud Station ist ideal für Dokumente, kleine Bildersammlungen und alles andere was man gemeinsam bearbeiten kann. Doch auch hier sollte man die Grenzen kennen und nicht die gesamte Dokumentenarchivierung verlegen. Denn alle Dateien werden von DS und PC/Mac regelmäßig auf Änderungen überwacht. Das kostet Leistung und ist ein Grund warum Synology die gleichzeitigen Verbindungen limitiert. Eine Möglichkeit seine Datenhaltung zu hinterfragen wäre z.B.: Wie oft werden die Daten außerhalb der Reichweite der DS benötigt? Weniger als ein Mal pro Woche? Oder gar pro Monat? Da wird schnell klar ob man die Daten wirklich überall mit hinnehmen muss.

Für Mobilgeräte gibt es die App „DS cloud“. Dort lässt sich zusätzlich konfigurieren, welche Dateien (Videos, Musik, …) bis zu welcher Größe synchronisiert werden sollen. Wenn man also mal eben einen selbstgemachten Film verteilen möchte, kann man das Mobilgerät davon ausnehmen. Etwas restriktiver ist die Mobil-App dafür bei der Wahl des Speicherortes.

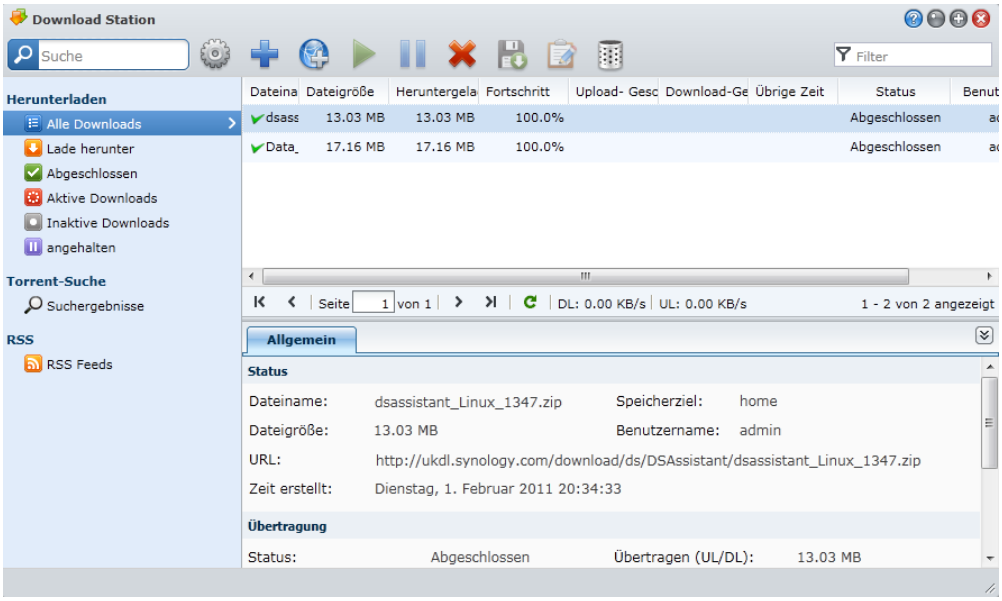
2.9 Download Station

Wer gerne größere Dateien aus dem Internet lädt und den eigenen Rechner nicht extra für längere Zeit laufen lassen will, kann mit der separaten Download Station Dateien automatisiert downloaden. Dabei werden auch verschiedene Protokolle wie zum Beispiel das Laden von einem Torrent unterstützt. Zum Nutzen der Download Station muss diese allerdings zunächst aktiviert werden und man benötigt einen Nutzer, welcher die Download Station verwenden darf (Untermenü „Anwendungen“, Benutzernamen und Passwort mit Manager/FileStation identisch).

Darüber hinaus sind auch Downloads aus folgenden Quellen möglich: RSS, NZB, eMule, ftp/http mit Authentifikation und von diversen Filehostern und Webplattformen wie Rapidshare oder auch Youtube (Free- und Premium-Accounts, je nach Dienst verschieden). Um unabhängig von der Firmware-Version auf Änderungen der Filehoster reagieren zu können, setzt Synology ein eigenes System inkl. Update-Mechanismus ein. Die Schnittstellen können über ein Menü einem einfachen Update unterzogen werden, sofern Synology eine angepasste Version anbietet. Die Suchfunktion dient dem Auffinden von Torrents in den konfigurierten Suchmaschinen.

In den Einstellungen kann genau festgelegt werden, wann wie viel heruntergeladen werden soll. Außerdem lässt sich die Bandbreite (auch mittels Zeitplan) verschieden steuern um beispielsweise Abends keine störenden Downloads zu haben, Nachts aber die volle Bandbreite auszunutzen.

Apropo Bandbreite: Bei mehreren Torrents gleichzeitig ohne Bandbreiteneinschränkung sollte man nicht auf die Idee kommen zeitgleich im Internet zu arbeiten oder Videos anzusehen. Denn die DiskStation kann die vorhandene Bandbreite diesbezüglich sehr gut auslasten …



2.10 Audio Station

Die Audio Station bietet als Gegenstück zur Photo Station Musik über das Netzwerk an. Über eine Oberfläche werden damit drei verschiedene Arten von Zielgeräten bedient. Zunächst kann man die

Musik ganz einfach über den Browser abspielen. Benötigt wird dafür nur ein Browser mit Flash. Der Format-Support ist nativ (also das was das Flash-Plugin wiedergibt) sehr beschränkt, viele inkompatible Formate können jedoch vor Transport über das Netzwerk entsprechend in Echtzeit umgewandelt werden.

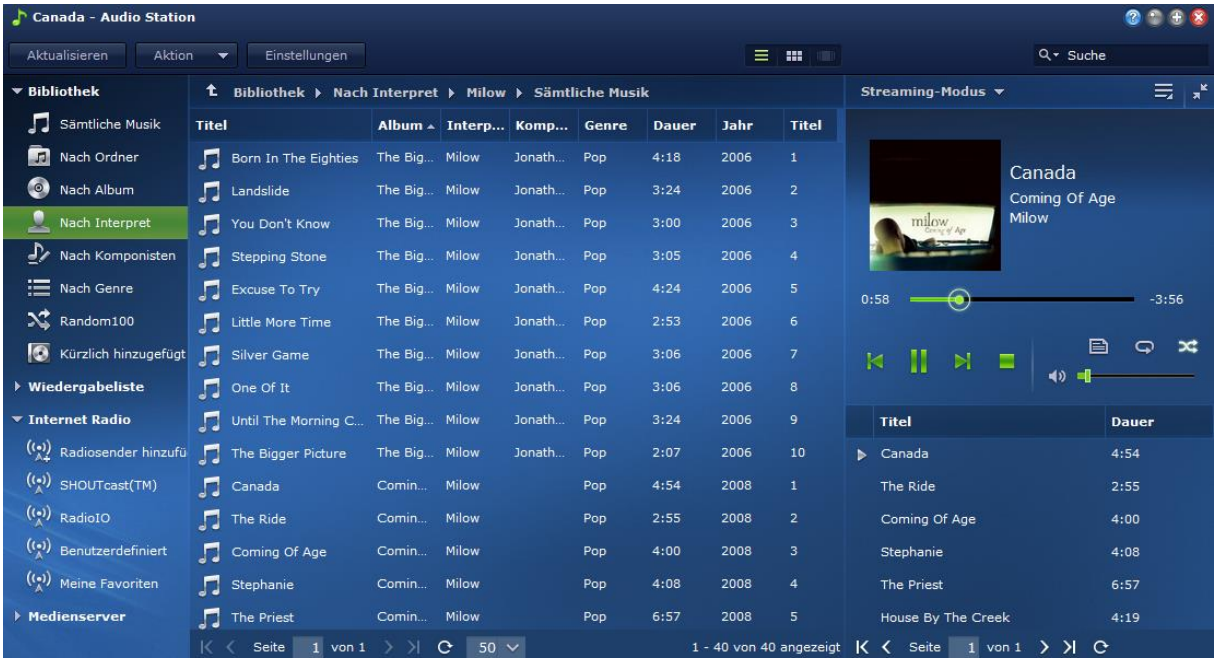
Als zweites bieten sich USB-Lautsprecher an. Synology vertreibt eine eigene externe Soundkarte in Verbindung mit einer Fernbedienung, doch auch viele andere Geräte sind laufen problemlos. Über die Weboberfläche ausgewählte Musik kann dann direkt ausgegeben werden.

Die dritte Möglichkeit bezieht sich auf Netzwerkgeräte. Das sind DLNA/UPnP und AirPlay-kompatible Abspielgeräte, im DLNA-Kontext „Medien-Renderer“ genannt. AirPlay bietet auch Multi-Raum Betrieb an (Wiedergabe von Musik gleichzeitig an mehrere Endgeräte). Die Audio Station tritt dabei als „Fernbedienung“ auf, inwiefern die Geräte die Unterbrechung oder Manipulation der Auswahl zulassen ist vom Gerät selbst abhängig.

Die Musik muss für die Audio Station innerhalb von „music“ liegen, als Pendant zu „photo“ und „video“ für die anderen Medien. Ebenfalls als Quelle geeignet sind andere DLNA/UPnP-Medienserver. Außerdem sind einige Internet-Radiosender bereits vorkonfiguriert.

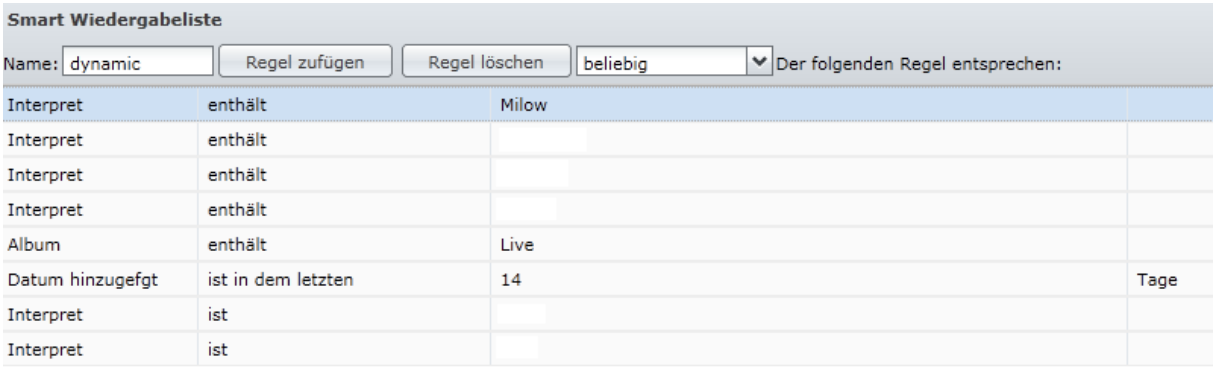
Abrundend sind dann noch der Editor für Metadaten (Titel, Album, …) und eine Anzeige von Lyrics zu nennen, sowie eine grobe Rechteverwaltung für Funktionen wie das Herunterladen einzelner Titel.

Für mobile Endgeräte steht DS audio als App zur Verfügung; auch hier können alle Arten von Endgeräten verwendet werden.



2.10.1 Smart(e) Wiedergabelisten

Synology nennt diese Funktion offiziell „Smart Wiedergabeliste“ und meint damit eine klassische Wiedergabeliste die ihren Inhalt dynamisch anhand bestimmter Regeln erstellt. Diese Regeln können sich an so ziemlich allem orientieren, was ein Lied an Tags mit sich bringt: Interpret, Album, Titel, Datum hinzugefügt, Dateipfad, Bitrate, Jahr und Genre. Hinzugefügt und konfiguriert werden sie ausschließlich über die Audio Station.



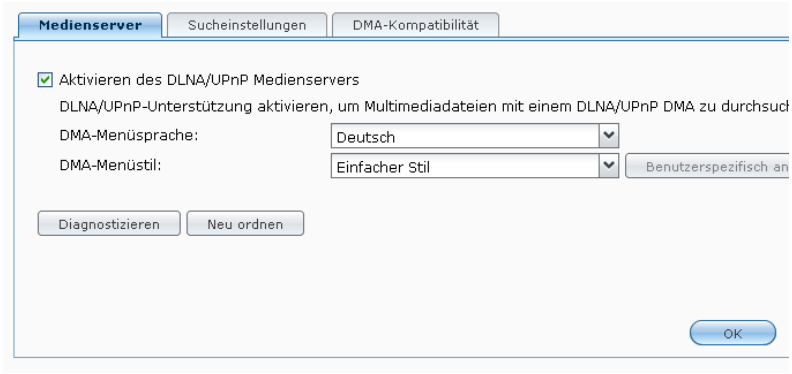
2.10.2 AirPlay

Eine Apple-spezifische Funktion zum Streamen ähnlich DLNA ist AirPlay, der Nachfolger von AirTunes. Nutzern von Apple-Geräten erleichtert diese die Verteilung von Medieninhalten sowie die Fernkontrolle der zugehörigen Abspielgeräte.

Die Audio Station stellt die Funktionen als „Medien Renderer“ bereit. Über der Anzeige des momentan abgespielten Liedes befindet sich eine Auswahl welche normal auf „Streaming-Modus“ steht. Dort lässt sich auf „Medien Renderer“ wechseln um andere kompatible Geräte zu kontrollieren. Als Besonderheit können hier mehrere Geräte mit einem Musik-Stream versorgt werden, was ein einfaches Mehrraum-System ermöglicht.

2.11 DLNA-Medienserver

Der DLNA-Server ist im Heimnetzwerk für die Verteilung von Medien (Fotos, Videos, Musik) zuständig. Der Name DLNA geht auf eine Dachorganisation zurück (siehe auch Kapitel 1.7.9) und steht für eine genauer spezifizierte Version von UPnP. Dass auch dessen Grenzen offenbar noch nicht eng genug sind zeigen die vielen Erweiterungen von Wiedergabegeräten. Da jeder Hersteller DLNA etwas anders interpretiert und implementiert, ist es nicht einfach zu allen Geräten kompatibel zu sein. Synology steuert diesem Verhalten mit der „DMA-Kompatibilität“ gegen. Dort sind verschiedene Profile hinterlegt, die dann (meist automatisch) den Geräten zugeordnet werden. Die Profile enthalten Informationen zu herstellerspezifischen Funktionen.



Bei Kompatibilitätsproblemen lohnt es daher, ein wenig mit diesen Profilen zu experimentieren. Auch nach einem Update des wiedergebenden Gerätes kann ein Profil Probleme machen. Sollte alles experimentieren nicht helfen, bleibt nur eine Kontaktaufnahme mit dem Hersteller des Gerätes und Synology.

Auch die Unterstützung der genauen Formate ist gerade bei Videos ein häufiges Problem. Hierfür ist der Hersteller des Wiedergabegerätes „zuständig“. Kommt dieser mit den Videos nicht zurecht, ist ein NAS meist machtlos. Selbst eine problemlose Wiedergabe über USB ist keine Garantie für Abspielen via Netzwerk.

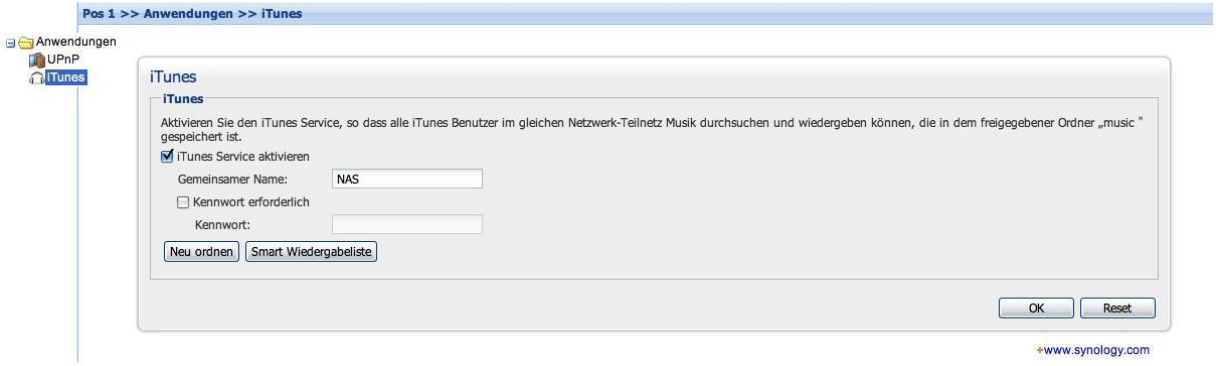
2.12 iTunes-Server[28]

Was kann der iTunes-Server und was kann er nicht?

Der iTunes-Server ist als Streaming-Server konzipiert und ermöglicht allen Rechnern mit installierten iTunes den Zugriff auf die Musikinhalte des Ordners „music“. Er ist dabei als reiner Lieferer eines Musik-Streams gedacht, welcher mittels der in den Musikdateien enthaltenen „ID-Tags“ die Inhalte auf den Clients zur Anzeige bringt (bei fehlenden Album-Tag nimmt er den Ordnernamen als Tag). Er ist nicht zum Verwalten der Musik mittels einer Bibliothek oder ähnlichem ausgelegt. Das heißt auch, dass mit ihm kein synchronisieren mit einem IPod möglich ist!

Wie richte ich den iTunes-Server ein?

Als erstes öffnet man den DSM und aktiviert unter iTunes den entsprechenden Dienst. Hierbei wird automatisch ein Ordner „music“ erstellt, welcher mittels der Rechtevergabe in „Gemeinsame Ordner“ wie die anderen Ordner für den Zugriff zu konfigurieren ist.

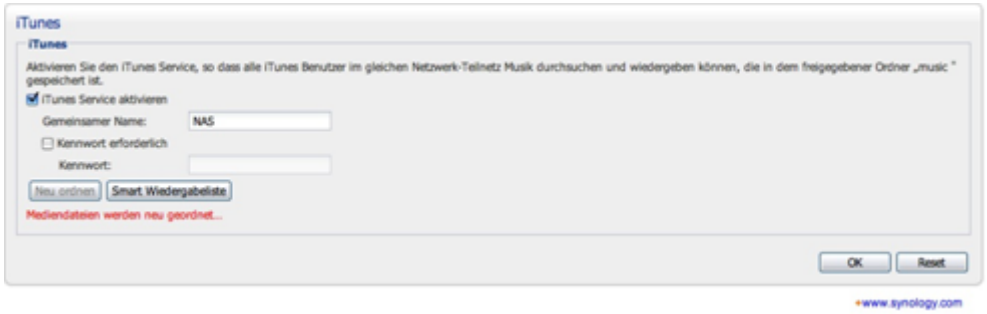


„Gemeinsamer Name“ bezeichnet, unter welchem Namen die Musik später im iTunes zur Verfügung stehen wird.

Sollte man ausschließen wollen, dass jeder der Nutzer des Netzwerkes Zugriff auf die Musik erlangen soll, kann auch ein Passwort vergeben werden.

Sobald Musik in den Ordner gelegt wird, beginnt die DS mit der Indexierung entsprechend der in den Dateien vorhandenen Tags. Zu erkennen an der roten Schriftzeile:

[28] Auch an dieser Stelle noch einmal ein Dankeschön an ag_bg welcher diesen Abschnitt verfasst hat.

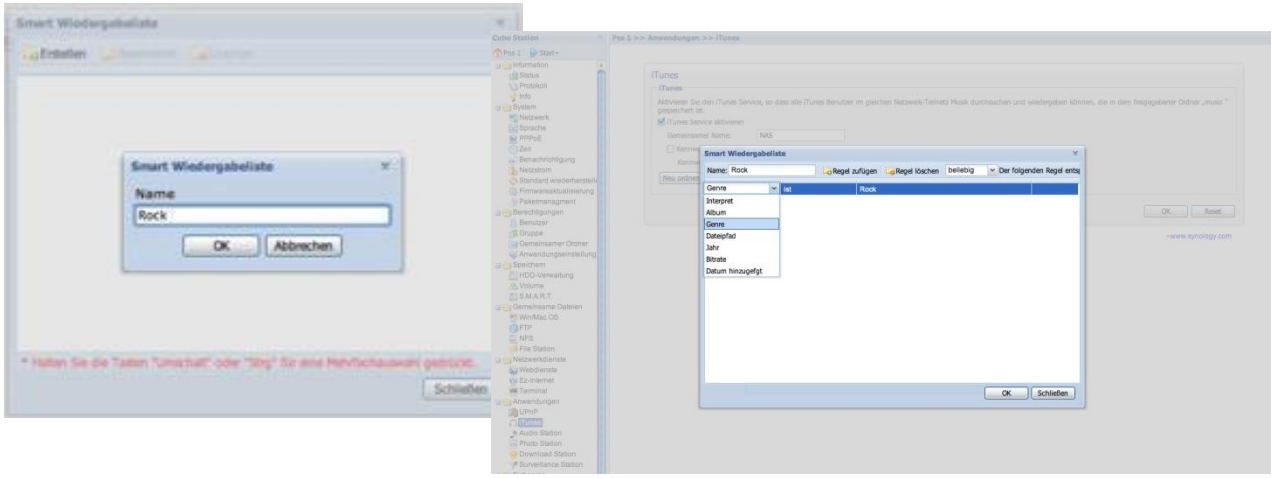


Wer gerne bereits vordefinierte Filter nutzt, kann im Management eine passende „Smart Wiedergabeliste" erstellen, welche ständig innerhalb des Ordners „music" nach neuen Dateien Ausschau hält, die eben die dort getroffenen Filter-Kriterien erfüllen.

Hier nun ein Beispiel:

Wir wollen alle Musik mit dem Genre Rock als gesonderte Liste angezeigt bekommen.

Smart Wiedergabeliste auswählen-> Erstellen und Name vergeben, Regel hinzufügen und in dem folgenden Menü die Einstellung entsprechend vornehmen (Wenn man mehrere Kriterien auswählen möchte, einfach die nächste Zeile mit dem folgenden Kriterium bearbeiten) und mit OK bestätigen. Die folgende Frage sollten sie mit „Ja" beantworten und das Fenster schließen, wenn Sie keine weiteren neuen Filter einrichten wollen. Anschließend einmal „Neu Ordnen" auslösen, damit die Wiedergabeliste auch passend eingearbeitet wird.

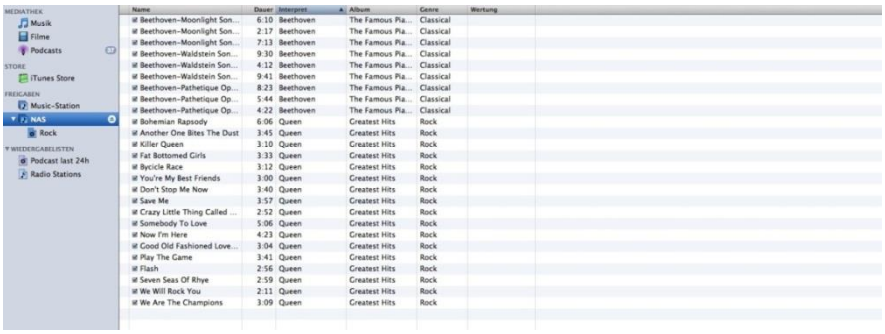


Allgemeiner Hinweis: Je mehr Smart-Wiedergabelisten erzeugt werden, umso mehr ist die DS mit der Filterung der Kriterien beschäftigt, welches längere Ladezeiten beim jeweils ersten Zugriff (einer jeden Nutzung) zur Folge hat, da diese Listen jedes Mal neu eingeladen werden müssen!

Damit haben wir auch schon die Funktionen des Servers abgearbeitet.

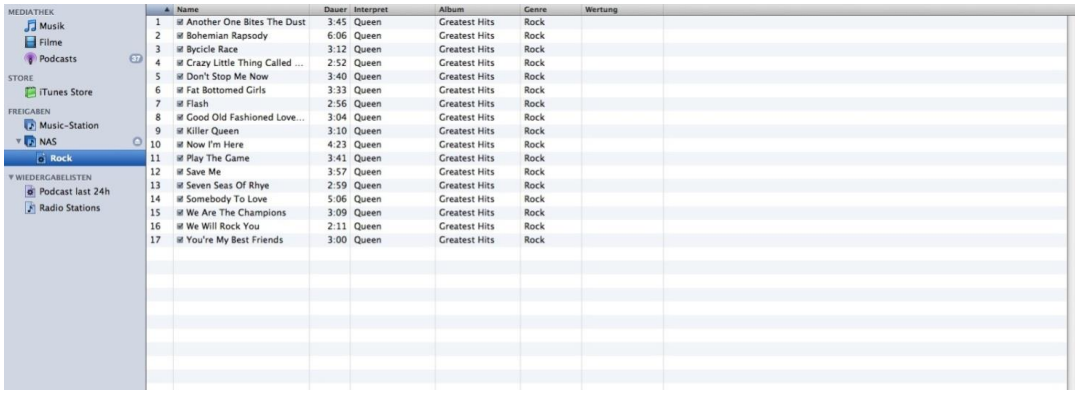
Kommen wir zum Client iTunes:

Innerhalb iTunes wird unsere DiskStation als Freigabe angezeigt mit dem vorher gewählten Namen (hier NAS).

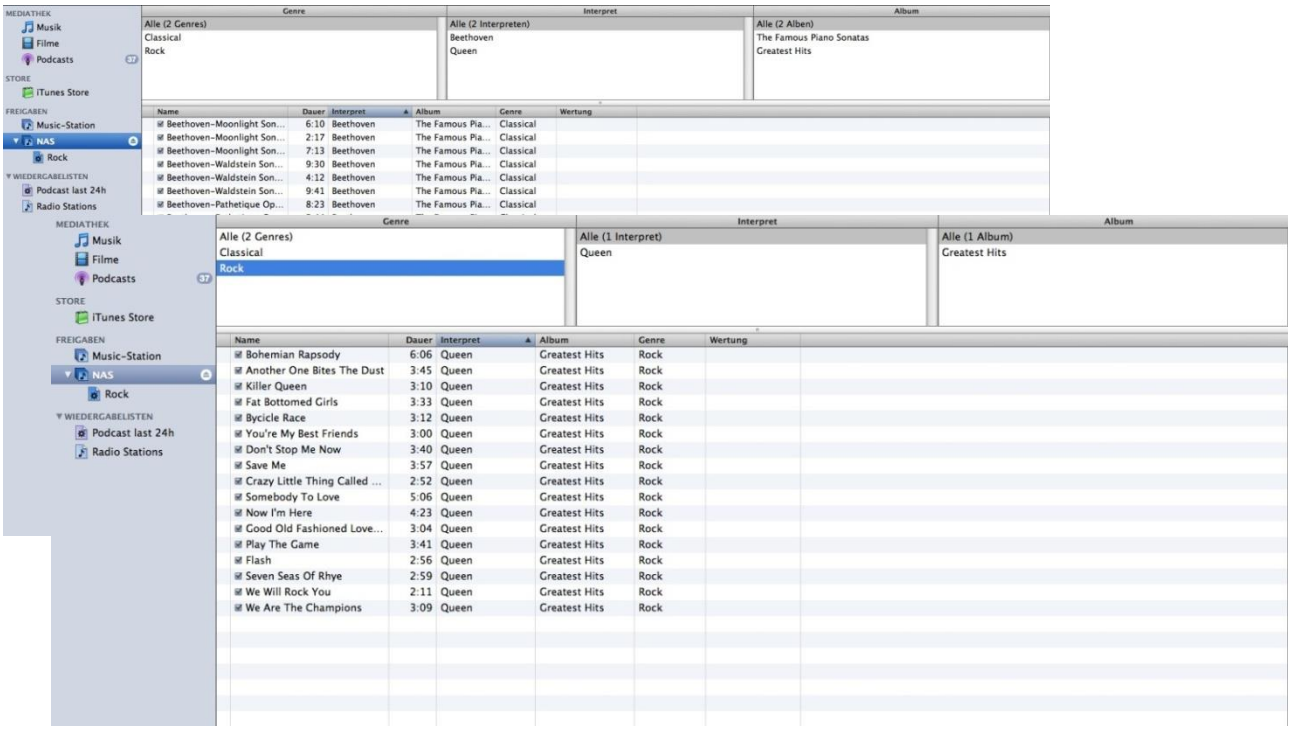


Wenn man nun auf diese Freigabe zugreift, wird der Inhalt des Ordners „music“ nach dem Stand der Indexierung angezeigt. Durch klicken auf das, links daneben befindliche, Dreieck werden die vorher erstellte Wiedergabelisten angezeigt.

So sieht dann unsere fertige Wiedergabeliste aus:



Als Alternative zum Anlegen von Wiedergabelisten sei noch auf den Übersichtsfilter aufmerksam gemacht, welcher durch Anklicken bestimmter Filter sowohl beim Abspielen als auch bei der Suche Behilflich sein kann (STRG-B oder Apfel-B).



Allgemein empfiehlt es sich sehr, seine Musikdateien mit den richtigen Merkmalen/Tags (Interpret, Album, Genre, …) zu versehen, da nur so eine hohe Übersichtlichkeit bei der Nutzung garantiert ist!

Unterstützte Formate sind:
MP3, M4A, M4P

und ohne Anzeige von Merkmalen:
WAV, AIF

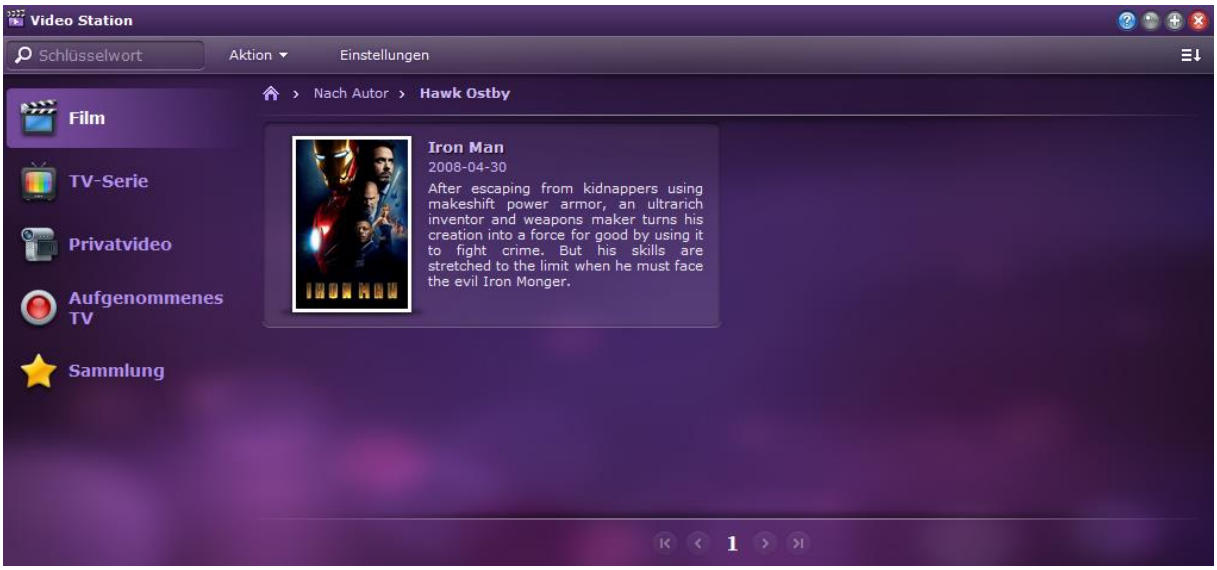
Ebenso werden Playlisten in den Ordnern unterstützt in folgenden Formaten:
M3U, WPL

Bevor ich dieses Thema schließe, noch kurz ein paar Worte zur iTunes-Alternative „Windows Media Player“ für PC-Nutzer. Dazu gibt es keinen offiziellen Dienst, doch das Bereitstellen von Musik ist auch hier ohne Probleme möglich. Zunächst erstellen wir einen Ordner auf unserer DiskStation und vergeben die entsprechenden Rechte. Dann beladen wir ihn mit Musik und fügen ihn als Netzlaufwerk hinzu. Nun kann man den entsprechenden Ordner zur Medien-Bibliothek hinzufügen.

2.13 Video Station

Die Video Station komplettiert die Medienverwaltung um nun nach Fotos und Musik auch Videos zu erfassen. Eine zentrale Funktion ist hierbei der Import von Metadaten aus einschlägigen, öffentlichen Datenbanken. Voraussetzung hierzu ist jedoch, dass Serien, Filme und Privataufnahmen separat gespeichert werden. Zur Einrichtung muss man der Video Station eben dies nämlich mitteilen und muss sich dabei auf einen Typ festlegen. Sollten die Metadaten nicht vorliegen oder falsch zugeordnet werden, ist auch eine Suche per Hand möglich. Wenn man beim Benennen der Dateien etwas aufpasst, geht das aber fast immer automatisch.[29]

Außerdem kann man über einen DVB-Stick (auf Kompatibilität achten!) die eigene Sammlung auch schnell vergrößern. Diese Funktion wird über die elektronische Programmzeitschrift „EPG“ gesteuert.

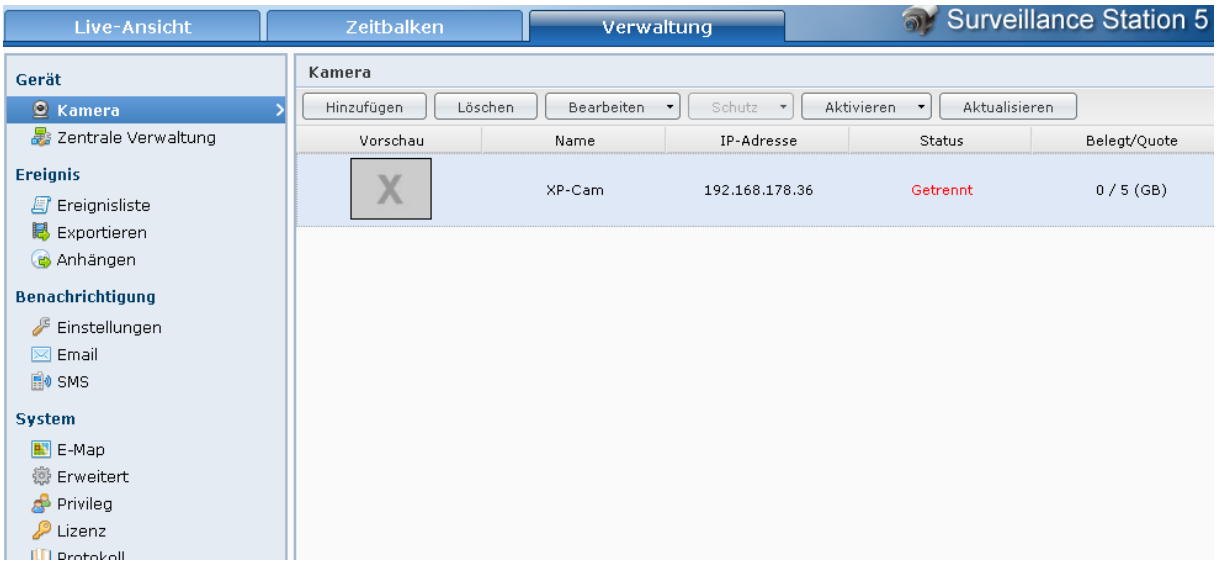


[29] Die empfohlenen Schemata sind hier beschrieben:
http://forum.synology.com/enu/viewtopic.php?t=59186#p225968

2.14 Surveillance Station

Wer sein Zuhause auch von der Arbeit aus im Auge behalten möchte, oder einfach nur seiner DiskStation beim Betrieb zusehen mag, der kann eine IP-Kamera in sein Netzwerk einbinden und auf diese von überall zugreifen (Kompatibilität beachten!). Auch wird von Synology ein Kamera-Limit gesetzt, welches durch den Zukauf von sogenannten „Lizenzen“ aufgehoben werden kann.

Wer mehrere DiskStations einsetzt, kann die Verwaltung der Surveillance Station außerdem zentralisieren, also alles von einer DiskStation aus administrieren.



2.15 E-Mail-Server

Als Ergänzung zum E-Mail-Server gibt es das Paket Mail Station bei Synology als *.spk-Paket zur Installation über das Paketmanagement – es enthält eine Weboberfläche zum Betrachten und Senden von Mails.

Sehr häufig taucht im Forum die Frage auf „Wozu der Mail-Server?“. Vorneweg: Er bietet keine großen Vorteile gegenüber einem „normalen“ E-Mail-Anbieter. Vielmehr haben die Synology-Entwickler damit auf die Wünsche der Community reagiert. Eigentlich ist es aber mehr eine nette Zugabe als ein wichtiges Tool. Für viele dürfte das eigenständige Verwalten der Mails eher Nachteile bringen. Denn um Dinge wie Backup, Sicherheit und Spam-Abwehr kümmern sich sonst meist die Provider. Die Mails jedes Nutzers werden in einem eigenen Unterordner des home-Verzeichnisses abgelegt und daher auch mit jedem Standard-Backup gesichert. Auch eine rudimentäre Spam-Abwehr ist vorhanden. Über die Kommandozeile lässt sich diese (unter der Haube läuft SpamAssassin) auch deutlich besser einstellen. Sicherheit und Verfügbarkeit stellen da allerdings eine ganze Reihe von Problemen dar, welche nicht ohne weiteres zu lösen sind. Jede Mail die durch das WWW rast und kein Ziel findet, etwa weil der Server gerade offline ist, verschwindet mitten im Nirgendwo. Abhilfe kann da ein „Mail-Spool“ schaffen. Ein einfaches Beispiel findet sich im nächsten Abschnitt. Der erste Schritt um die Sicherheit der DS zu gewährleisten, ist wie immer die Verschlüsselung aller Übertragungen. Genauere Informationen dazu finden sich im ersten Kapitel bei

den jeweiligen Mail-Übertragungs-Protokollen. Des Weiteren ist eine Viren-Abwehr [30] empfehlenswert um schädliche Dateien fern zu halten.

Doch natürlich bringt die Mail Station auch Vorteile mit sich. So können sie ihre Mails von verschiedenen Anbietern auf einer Oberfläche verwalten, wenn zusätzlich das Mail Station-Paket installiert ist. Auch dauert das Abrufen der Mails kaum noch ein paar Sekunden. Schließlich können sie mit ihrem Mail-Server nun über Gigabit statt nur einer DSL-Verbindung kommunizieren.

Apropos: Das Paket „Mail Station“ von Synology, welches sich über das Paketmanagement einspielen lässt, enthält zusätzlich mit Roundcube eine Weboberfläche auf der einiges konfigurierbar ist: Das Abholen von anderen POP3-Servern, das Versenden von Mails welche über die Weboberfläche geschrieben werden über die SMTP-Server der Provider, …

Noch ein kleiner Hinweis: Nur kleine Buchstaben werden als Mail-Adresse akzeptiert. Bitte beim Einrichten der Benutzer beachten! Das ist kein Mail Station-Problem sondern eine generelle Regel im WWW, die viele Anbieter jedoch ignorieren und korrigieren indem sie alles auf Kleinbuchstaben umschreiben.

2.15.1 Mail Station als vollwertiger Mail-Server mittels Relay

Dieser Abschnitt setzt das Vorhandensein eines kostenpflichtigen .de-DDNS-Accounts bei selfhost.de voraus. Andere Anbieter sind möglich, jedoch noch nicht dokumentiert.

Ein grundlegendes Problem ist, dass E-Mails, welche von dynamischen IP-Adressen empfangen werden, meist von den Spam-Filtern direkt gelöscht werden.

```
<matthieu-ds@hotmail.de>: host mx1.hotmail.com[65.55.37.88] said: 550 DY-001
    Mail rejected by Windows Live Hotmail for policy reasons. We generally do
    not accept email from dynamic IP's as they are not typically used to
    deliver unauthenticated SMTP e-mail to an Internet mail server.
    http://www.spamhaus.org maintains lists of dynamic and residential IP
    addresses. If you are not an email/network admin please contact your
    E-mail/Internet Service Provider for help. Email/network admins, please
    visit http://postmaster.live.com for email delivery information and support
    (in reply to MAIL FROM command)
```

Um dies zu verhindern müssen unsere Mails daher einen kleinen Umweg nehmen:

Zunächst erstellen wir uns einen **kostenpflichtigen** Account mit DDNS bei selfhost.de. Dieser bietet aber auch einen weiteren entscheidenden Vorteil: Ist die DiskStation aus welchem Grund auch immer offline, würde normal die Mail in den Unweiten des Internets verschwinden. Selfhost.de wiederum speichert Ihre Post, bis der Server sich zurück zur Arbeit meldet. Auf diese Weise geht garantiert nichts verloren.

Zuerst beginnen wir mit unserer Arbeit direkt an der Mail Station und wählen diese im DSM aus. Dort geben wir als Domainname die neue DDNS-Adresse an. Bei allen anderen Optionen setzen wir einen Haken.

[30] Ein möglicher Ansatz wäre das spk „Rootkit Hunter“.

Nun loggen wir uns bei selfhost.de ein und legen einen neuen Mailspace über „Account -> Mail Admin“ an. Dort dann Spool anklicken und unsere DDNS-Adresse auswählen. Jetzt noch die Daten, welche hinter „Username(fest)“ und „Passwort“ stehen notieren, damit wir sie später übernehmen können und zu guter Letzt mit einem Klick auf „ändern“ bestätigen.

Jetzt geht die Arbeit an der DiskStation los. Wir öffnen unseren SSH/Telnet-Client (z.B. Putty) und beginnen:

```
cd /usr/syno/Mail Station/etc
cp main.cf main-backup.cf
vi main.cf
```

In der gerade geöffneten Datei müssen wir jetzt bis zum Ende und fügen hinzu:

```
# selfhost
relayhost = [mail.selfhost.de]
smtp_sasl_auth_enable = yes
smtp_sasl_password_maps = hash:/usr/syno/Mail Station/etc/smtp_auth
smtp_sasl_security_options = noanonymous

smtp_use_tls = yes
smtp_enforce_tls = yes
smtp_tls_enforce_peername = no

myhostname = eure Domain
smtp_sasl_auth_enable = yes
```

Nun öffnen wir eine neue Datei:

```
vi smtp_auth
```

Jetzt kommen unsere Zugangsdaten, welche wir auf den Zettel geschrieben hatten, zum Einsatz:

```
mail.selfhost.de USER:PW

(z.B. mail.selfhost.de postmaster@masdasdoi.mail.selfhost.de:SDz78sJHD)
```

Nun muss noch die Datei in ein für die DiskStation lesbares Format umgewandelt werden:

```
/usr/syno/Mail Station/sbin/postmap smtp_auth
```

Damit wäre die Arbeit an der DiskStation beendet und wir können unseren neuen Mail-Server nutzen. Wer will, kann natürlich auch mit Outlook auf die Mails zugreifen. Für jeden Nutzer, der auf dem DSM erstellt wurde, existiert jetzt ein Mailkonto. Die POP3 und SMTP-Zugänge sind schlicht und einfach die DDNS-Adresse.

2.16 DDNS und QuickConnect

Um DDNS einzusetzen, besitzt die DS natürlich auch einen eigenen Clienten. Man kann damit seine IP bei mehreren Anbietern updaten. Synology hat dazu die Daten von verschiedenen Servern integriert. Leider ist das Abgleichen mit anderen Anbietern schwierig. Auch hat die DS einen entscheidenden technischen Nachteil: Anders als ein Router bemerkt eine NAS nicht automatisch, wenn sich die IP ändert. Also kontaktiert der Client in regelmäßigen Abständen einen Synology-Server. Ein Router hingegen kann in Sekundenschnelle reagieren, sobald er eine neue IP vom Provider erhält. Hat man daher die Wahl und der Router unterstützt DDNS, ist es besser, dem Router entsprechendes zu

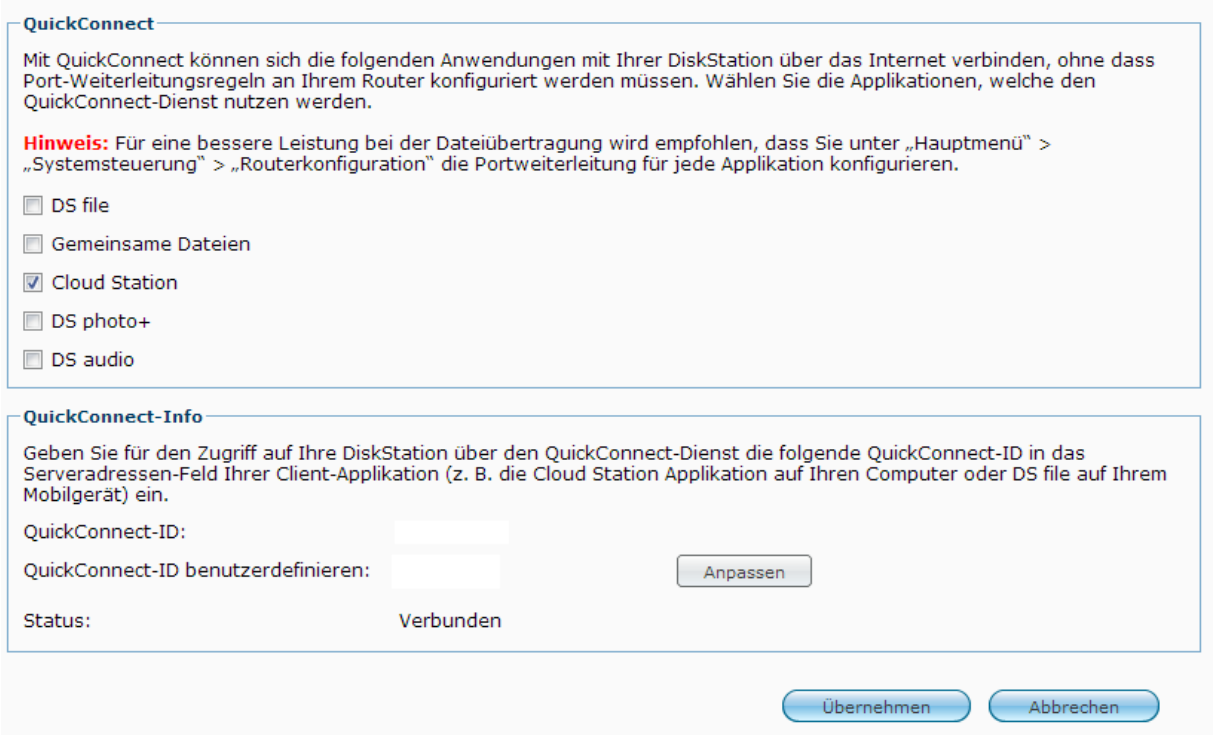
überlassen. Auch unterstützen diese meist mehr Anbieter. Doch es kommt noch besser: Es ist bereits vorgekommen, dass ein Nutzer von dyndns.com abgemahnt wurde, weil die Techniker mehrere Clients unterscheiden konnten und daher Manipulation vermuteten. Somit sollte immer nur einer die Übertragung vornehmen.

Wem die wenigen Optionen nicht ausreichen, der kann sich QTips „ddnsupdater“ anschauen, welcher über das Community Package Hub Projekt[31] zur Verfügung steht.

2.16.1 QuickConnect (ID)

So viel zum traditionellen Ansatz. Es gibt allerdings auch einige Szenarien in denen DDNS und Portfreigaben nicht in Frage kommen, z.B. weil man keine richtige externe IP bekommt sondern sich diese mit anderen Nutzern teilt (bei Funkverbindungen üblich). Für diesen Fall hat Synology einen Relay-Dienst eingerichtet. Eine dafür konfigurierte DiskStation meldet sich regelmäßig bei Synology und fragt ob jemand Interesse an einer Verbindung hat. Wenn man mit einer mobilen App oder einem anderen QuickConnect-fähigen Programm zugreifen möchte, liefert Synology dann die Verbindung „huckepack“ an die DiskStation aus. Damit sieht es für beide so aus als hätten sie die Verbindung initiiert und NAT und Firewalls sind kein Problem mehr. Alle weiteren Daten werden aber direkt zwischen Anwender und DiskStation ausgetauscht.

Welche Applikationen QuickConnect nutzen dürfen lässt sich auch im DSM einschränken.



2.17 Grundlegendes zum Thema Sicherheit

Hierbei handelt es sich zwar nicht um einen Bestandteil der Firmware, doch bevor wir im nächsten Kapitel die Backups behandeln, müssen wir uns erst einmal ein wenig die Sicherheit unserer Daten ansehen. Sie glauben mir nicht? Öffnen sie doch einmal die FTP-Ports und schauen sie nach ein paar Tagen in ihr Verbindungsprotokoll. Mittlerweile werden sie eine ganze Menge von Einträgen vorfinden welche besagen, dass jemand versucht hat ihr Passwort zu umgehen. Meist wird dabei die

[31] Siehe http://package.10trum.de/

„Brute-Force“-Methode verwendet. Mit anderen Worten: In möglichst kurzer Zeit werden so viele Passwörter wie möglich ausprobiert. Vorausgesetzt, der Benutzername stimmt, erhält der Hacker am Ende das richtige Passwort. Nur das ist genau was wir nicht möchten. Doch wir beginnen nicht an der DiskStation selber.

Zunächst beschäftigen wir uns mit dem Router. Diesen sollte man mit einem guten Passwort schützen und nicht vom Internet aus erreichbar machen. Darüber hinaus ist es wichtig, dass der Router eine eigene Firewall besitzt. Ist dies nicht der Fall, sollte man einen anderen Router in Betracht ziehen oder die Firewall der DS einschalten. Als nächstes müssen wir damit beginnen Löcher in die Firewall zu schlagen. Wir sind bei den Ports angelangt. Hierbei gilt die simple Regel: So wenig wie nötig, so effizient wie möglich. Bevor sie sich jetzt die lange Port-Liste von Synology heranziehen und beginnen diese abzutippen, halten sie bitte inne. Zunächst überlegen sie, welche Dienste sie genau von überall nutzen möchten. Wenn sie die Download Station nicht brauchen, sollten die entsprechenden Ports genauso unberührt lassen, wie wenn sie die Audio Station ausschließlich übers LAN betreiben. Als zweites schauen sie, ob es auch eine verschlüsselte Alternative gibt. So grenzt es an grobe Fahrlässigkeit die Ports für die Administrationsoberfläche per http zu öffnen. Wenn sie wirklich Zugang übers Internet brauchen, wählen sie lieber Port 5001 für https. Dasselbe gilt für alle anderen Dienste wie den Webserver und insbesondere Telnet. SSH hingegen können sie durchaus freigeben(Telnet 23, SSH 22), wenn die „Automatische Blockierung“ aktiviert ist. Nun sollte sich ihre Liste sehr verringert haben. Schließlich können sie nun mit dem abtippen in die Liste der Portfreigaben ihres Browsers beginnen. Für genaue Informationen zu diesem Thema konsultieren sie bitte das Handbuch ihres Routers, da sich dieser Prozess bei verschiedenen Herstellern sehr stark unterscheidet.

Eine kurze Bemerkung noch zu IDS bevor wir uns vom Router entfernen. Diesen Schutz bieten nicht viele Router. Haben sie jedoch die Möglichkeit, sollten sie diese unbedingt nutzen. IDS kann den Zugriff auf das Netzwerk als aller erstes stoppen bevor es überhaupt ihr NAS erreicht.

Wie bereits angekündigt lassen wir jetzt den Router hinter uns und wenden uns der DiskStation zu. Zunächst werfen wir einen Blick auf die Liste der Benutzer und ihrer Rechte. Die DiskStation macht das Verwalten dieser recht einfach und effektiv. Geben sie ihren Nutzern nur so wenig Rechte wie wirklich nötig. Insbesondere bei den Schreibrechten ist Vorsicht geboten. Besser sie müssen diese später auf Nachfrage des Anwenders nachreichen. Fordern sie ihre Nutzer außerdem dazu auf, sichere Passwörter zu verwenden.

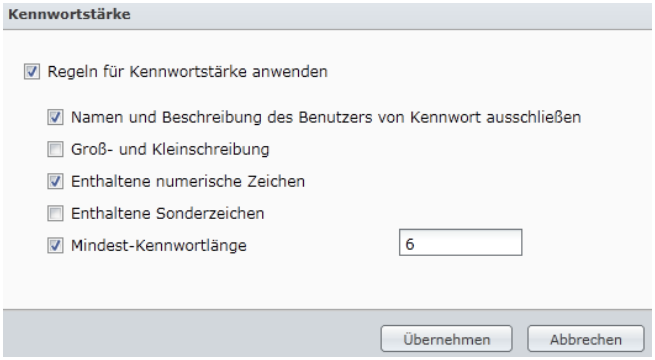
Ich habe vorhin bereits Brute-Force-Attacken erklärt. Seit den letzten Firmware-Updates bringt die DiskStation eine eigene Sicherung gegen dieses Vorgehen mit. Dabei werden IP-Adressen, welche sich innerhalb von x Minuten mindestens x Mal fehlerhaft versucht haben einzuloggen, auf eine Liste gesetzt. Bevor sich ein Nutzer verbindet, wird diese Liste überprüft und bei Übereinstimmung die Verbindung abgebrochen, unabhängig davon ob die Zugangsdaten falsch oder richtig waren. Diese „Automatische Blockierung“ muss zunächst aktiviert werden. Der FTP-Dienst bietet außerdem die Möglichkeit ausschließlich mit SSL/TLS verschlüsselte Verbindungen anzunehmen. Nutzt man FTP über das Internet, sollte man dies aktivieren. Beachten sie dann, dass ihr Programm, welches sie zum Zugang nutzen, dies unterstützt. (z.B. WinSCP). Ab dem DSM 2.2, kann dies sogar auf alle Dienste (also auch SSH, DSM, NFS, …) erweitern.

Wie man den Webserver absichert haben wir bereits mit den „.htaccess“-Dateien besprochen. Wer in seinem Router die verschlüsselten Ports aktiviert hat, muss nun außerdem die entsprechenden Funktionen im DSM aktivieren.

Einzelne Shares können auf der DS außerdem verschlüsselt werden. Dies würde bei Diebstahl des Gerätes den Diebstahl der Daten verhindern.

Zu guter Letzt möchte ich noch ein paar Worte über Passwörter sagen. Hacker-Angriffe basieren häufig auf Wörterbüchern, welche oft verwendete Wörter enthalten. Daher sollten sie nie Wörter in ihrem Passwort verwenden. Doch auch dies reicht bei weitem nicht aus. Ihr Passwort sollte nicht zu kurz sein (**6-8 Zeichen MINIMUM**) und **sowohl Zahlen als auch Buchstaben** enthalten. Um die Sicherheit weiter zu erhöhen empfiehlt es sich außerdem, **Sonderzeichen** zu verwenden. Denn je länger ihr Passwort ist und je mehr Arten von Zeichen es verwendet, umso mehr Kombinationen muss ein Hacker ausprobieren. Ein Passwort welches alle diese Hinweise berücksichtigt (z.B. 12 Stellen mit Zahlen, Buchstaben und Sonderzeichen sowie kein erkennbares Wort) sollte es einem Angreifer sehr schwer machen. Bitte erinnern sie auch ihre Nutzer über diese Gefahr, denn am Ende sind sie auch für deren Daten verantwortlich, Passwort hin oder her!

Wer jedoch den Benutzern nicht vertrauen möchte, kann die Passwortstärke selbst festlegen. In der Systemsteuerung unter „Benutzer“ gibt es ein entsprechendes Menü. Doch seien sie vorsichtig: Man kann Nutzer auf diese Weise auch gehörig nerven. Ein paar Einstellungen wie die Mindestlänge sind durchaus sinnvoll.



Doch auch der beste Sicherheitsschutz kann einmal Löcher haben, daher sollten sie sich auch die Themen Backup und Firewall ansehen.

2.18 Printserver (Drucker und Multifunktionsgeräte an der DiskStation)

Bestandteil jedes Heimnetzwerks ist häufig auch ein Drucker. Aber ebenso häufig muss dabei ein Windows-PC als Annahmestelle für Aufträge herhalten. Die DiskStation bietet aber auch einen sogenannten Printserver, der es ermöglicht, USB-Drucker an die DiskStation anzuschließen und diese dann im ganzen Netzwerk zu nutzen. Seit im DSM 3.1 auch Multifunktionsgeräte („MFP“) mit Scan und Fax unterstützt werden, muss zunächst der DSM geöffnet und bei den USB-Geräten die Art von Drucker gewählt werden. In neueren Windows-Betriebssystemen wird der Drucker auch in der Netzwerkumgebung angezeigt und kann per Doppelklick installiert werden – vorhandenen Treiber auf dem PC vorausgesetzt (Nein, der Treiber wird nicht auf der DS gespeichert). Andernfalls bleibt der Synology Assistant, der den entsprechenden Vorgang vereinfacht und begleitet.

Dabei besteht ein großer Unterschied zwischen der Implementation eines einfachen Druckers und der von Multifunktionsgeräten: Drucker werden über eine Linux-typische Schnittstelle eingebunden und über einen entsprechenden Server bereitgestellt. Also etwas, dass man theoretisch mit viel Aufwand auch mit jedem Linux-Rechner hätte bewerkstelligen können. Aber bei Multifunktionsgeräten packt Synology die ganze USB-Schnittstelle ein und bringt sie über einen

speziellen Treiber zum PC, der dann denkt der Drucker wäre direkt an ihn angeschlossen, obwohl das USB-Kabel ganz woanders endet.

2.18.1 AirPrint

Bei einigen Druckern wird außerdem das „AirPrint"-Protokoll von Apple unterstützt. Im Hintergrund verwendet Synology die Treibersammlung von „gutenprint"[32]. Dort unterstützte Drucker haben somit auch eine gute Chance auf AirPrint-Fähigkeit. Dennoch gilt hier:

Für alle hier beschriebenen Funktionen sollte man stets die Kompatibilitätslisten von Synology zu Rate ziehen.[33]

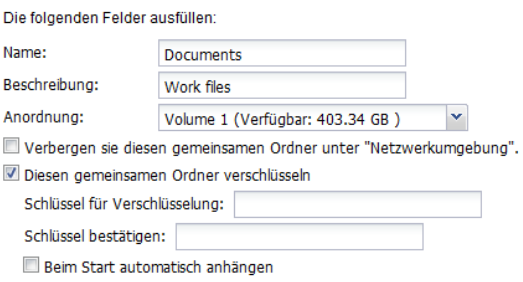
2.18.2 Google Cloud Print

Eine weitere Funktion greift auf die „gutenprint"-Treiber zurück: die Google Cloud Print[34]-Anbindung. Damit kann ohne Treiberinstallation via Internet gedruckt werden.

Wirklich interessant sollte Cloud Print vorerst aber nur für Nutzer von Googles Chrome OS sein. Mobil zu drucken geht auch über VPN in Verbindung mit den im LAN üblichen Methoden des Printservers.

2.19 Verschlüsselung

Um Daten beispielsweise gegen Diebstahl der Hardware (Festplatten) zu sichern, kann man seine Daten zusätzlich verschlüsseln. Doch man sollte die dabei entstehenden Performanceverluste berücksichtigen, auch wenn einige DS integrierte Hardwareunterstützung bieten. Auch wird man beim Aktivieren auf die Limitationen hingewiesen: Kein NFS, geringere Leistung und keine Rettung von Daten bei verlorenem Passwort. Außerdem müssen Sie sich vor jeder Nutzung einloggen und den Schlüssel angeben, wenn Sie nicht das „Automatische beim Start anhängen" aktivieren. Selbigen bekommen Sie außerdem als Datei zur Aufbewahrung. Die etwas unglücklich übersetzten Optionen „Anhängen" und „Trennen" sorgen für die Zugangsregelung und sperren die Daten bzw. geben sie wieder frei. Ein kleines Schloss in der Tabelle der „Gemeinsamen Ordner" symbolisiert den aktuellen Status.



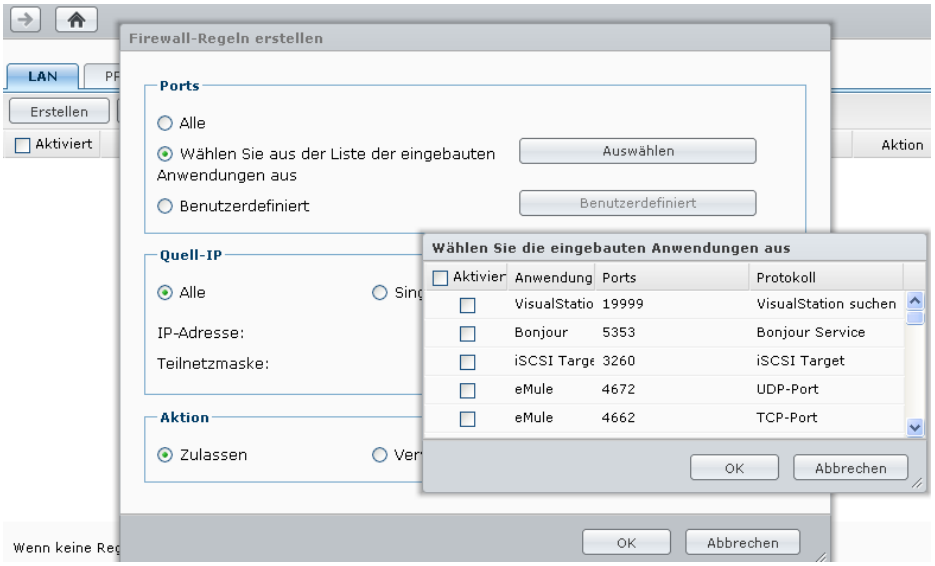
2.20 Firewall

Insbesondere wer seine DS mittels PPoE ohne Router und somit eigentlich ohne Firewall betreibt, wird sich über diese Funktion besonders freuen.

Die Oberfläche im DSM ist recht intuitiv gestaltet. Die meisten Router bieten ein ähnliches GUI. Beachten sollte man, dass die DS zwischen LAN und PPoE unterscheidet! Die Regeln müssen separat eingegeben werden. Ansonsten ist die DS-Firewall mit den Systemen der Router beinahe identisch. Vielen Routern voraus hat die DS außerdem eine Unterscheidung nach IP. Auch beachten sollte man die Einstellung am unteren Rand um festzulegen, was mit unbestimmten Ports passieren soll. Wem

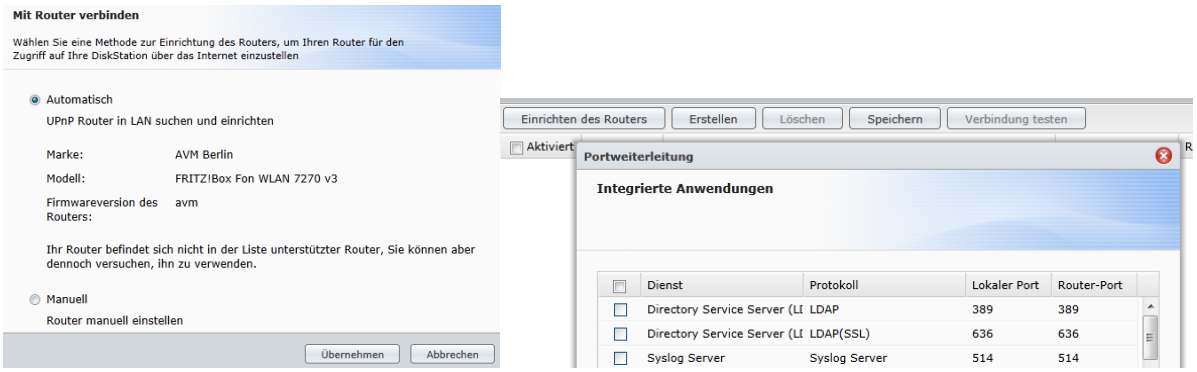
[32] Webseite: http://gimp-print.sourceforge.net/, erst ab Firmware 1742
[33] http://www.synology.com/support/compatibility.php
[34] Hilfe des Projekts mit vielen Infos über Funktionsweise usw.: http://www.google.com/support/cloudprint/
Google-Labs-Seite: http://code.google.com/intl/de-DE/apis/cloudprint/docs/overview.html

die einzelnen Ports zu kompliziert sind, der kann auch auf eine Liste mit allen Anwendungen zurückgreifen.



2.20.1 Routerkonfiguration

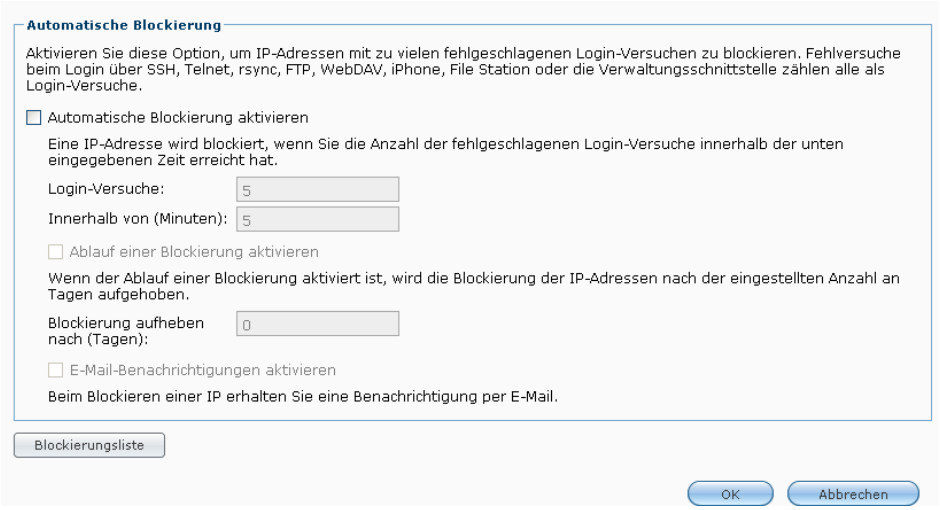
Um den Schritt zum Internetzugang komplett abzudecken, bietet Synology auch eine Konfiguration der Router-Firewall über den DSM. Dabei versucht die DiskStation zunächst selbstständig das Router-Modell zu ermitteln. Eine Auswahl von Hand aus der Datenbank von Synology ist aber auch problemlos möglich. Anschließend lässt sich die Firewall des Routers ähnlich der der DS kontrollieren. Wieder ist es möglich, Dienste je nach Anwendung oder nach von Hand angegebenem Port zum Internet zu öffnen. Wird der heimische Router hingegen noch nicht unterstützt, bleibt immer noch die herkömmliche Gangart über die Portfreigaben im Router (NAT).



2.21 Automatische Blockierung

Dies ist eine Erweiterung auf Wunsch von Nutzern, welche früher nur für den FTP-Server verfügbar war. Sie blockt den Zugang einer bestimmten IP nachdem diese versucht hat das Passwort mittels Brute-Force-Attacke zu „erraten“.

Wann genau eine IP geblockt werden soll, kann recht genau eingestellt werden. Auch das Löschen nach einigen Tagen ist problemlos möglich. Sollte man trotzdem mal eine eigene IP in der Liste haben, kann diese gezielt gelöscht werden. Diese Funktion ist dringend jedem zu empfehlen. Sie ist ein wichtiger Sicherheitsschritt.



2.22 Antivirus

2.22.1 Essential

Ein NAS auf Linux-Basis ist häufig kein lohnendes, direktes Ziel für Angreifer. Deutlich einfacher ist es aus Sicht selbiger Person, mittels eines infizierten PC/Mac auf einem Netzlaufwerk zu speichern. Darauf greifen andere Benutzer zu, halten die Daten für sicher und infizieren sich selbst.

Um dieses Szenario zu unterbinden, stellt Synology „Antivirus Essential“ über das Paketzentrum bereit. Es handelt sich dabei jedoch nicht um eine Eigenentwicklung. Als Grundlage dient das verbreitete ClamAV mitsamt seiner Engine und seinen Signaturen.[35] Im Fall eines Fundes werden alle Dateien zunächst in Quarantäne verschoben und können dann isoliert betrachtet werden. Dazu gibt es die üblichen Funktionen wie Protokoll und programmierbare Scans. Gegenüber kostenpflichtigen Anwendungen fehlen den „Essentials“ aber einige Details.

2.22.2 McAfee

Eine deutlich bessere Erkennungsrate mit aktuelleren Signaturen und einer schnelleren Engine bietet McAfee – gegen das in diesem Segment übliche Abo-Modell. Der Kauf eines solchen ein- oder mehrjährigen Abos läuft dabei über Synology und deren MyDS-Dienst. An diesen wird die Lizenz gekoppelt. Die Bezahlung übernimmt Paypal.

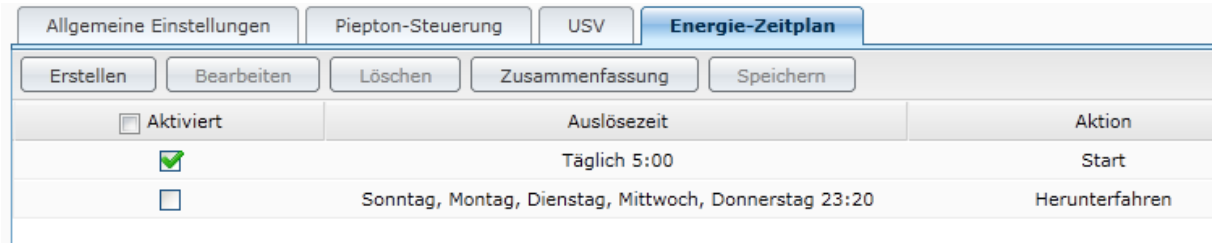
2.23 „Energie“

Unter dieser Überschrift kann man vieles positionieren. Bei Synology sind das USV, „Piepton-Steuerung“, Hibernation, Energie-Zeitplan und Lüftereinstellungen.

Der Energie-Zeitplan löste im DSM 3.0 endlich die einfache Steuerung des zeitlichen Hoch- und Herunterfahrens ab, denn diese konnte nur einen Zeitpunkt definieren, was bei vielen Nutzern auf

[35] Mit “/var/packages/AntiVirus/target/bin/synoavscan --showeng” kann man sich das verwendete Programm ausgeben lassen.

Unverständnis stieß. Der Nachfolger erlaubt hingegen viel größere Freiheiten. Für jeden Wochentag lassen sich problemlos mehrere Aufträge vergeben. Ein Klick auf „Zusammenfassung“ zeigt dann noch einmal alle Ereignisse einzeln an. Doch am wichtigsten ist es, danach „Speichern“ zu klicken.

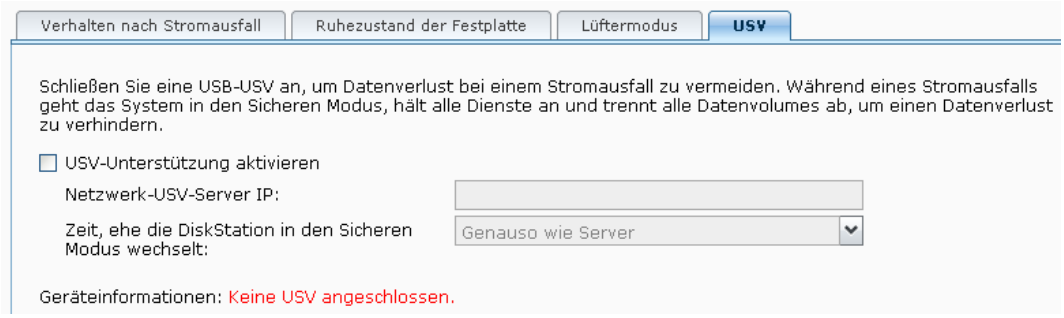


Die Lüftersteuerung ermöglicht eine Unterscheidung zwischen 2,5 und 3,5 Zoll-Festplatten sowie einen deaktivierbaren Warnton bei Ausfall des Lüfters. Im 2,5“-Modus werden die Lüfter auf niedrigeren Drehzahlen betrieben, da davon ausgegangen werden kann, dass weniger Wärme entsteht.

2.24 USV

Diese Notfall-Batterien („Unterbrechungsfreie Stromversorgung“) versorgen Geräte mit Strom falls ein Stromausfall gerade mal für Datenverlust sorgen möchte. Dabei wird die USV vor die Netzteile der zu schützenden Geräte geschalten. Damit diese jedoch bei Stromausfall auch bemerken dass der USV irgendwann die Luft ausgeht, werden diese mit USB oder speziellen Monitoring-Karten an die Geräte gekoppelt. Bei USB lässt sich aber nur ein Gerät mit der USV verbinden. Zu diesem Zweck kann ein Synology-Gerät als „USV-Server“ dienen und den Zustand der USV über das Netzwerk melden. Allerdings sollte man dabei wieder auf die entsprechende Kompatibilitätsliste achten.

Neigen sich die Ressourcen einer USV ihrem Ende, schaltet eine DS die meisten Dienste ab und hängt das Dateisystem aus. Obwohl prinzipiell noch erreichbar liefert eine DS in diesem Zustand keine Daten mehr und führt keine Aufgaben aus. In diesem Zustand besteht für Dateisystem und Daten keine Gefahr mehr.

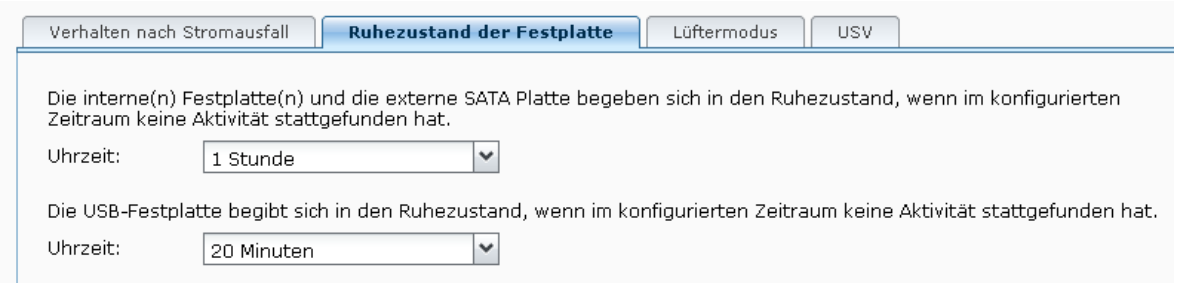


2.25 Hibernation

Diese Funktion ist insbesondere für Gelegenheitsnutzer interessant. Wer nicht rund um die Uhr seine DiskStation beschäftigt, kann deren Festplatten nach gewisser Zeit herunterfahren.

Aber: Wer seine DiskStation auslastet und doch Hibernation einschaltet, der kann sich damit auch seine Platten beschädigen. Zu häufiges starten und stoppen ist für diese anstrengender als ein Betrieb 24/7.[36]

[36] 24/7= 24h pro Tag, 7 Tage die Woche



2.25.1 Hibernation-Log

Dies ist eigentlich eine Funktion für den Support und das Debugging seitens Synology. Aber es ist häufig die einzige Möglichkeit um festzustellen, was eigentlich den Hibernation-Modus der Festplatten ständig stört. Diese Vorgehensweiße ist vor einiger Zeit aus einem internen Dokument von Synology durchgesickert.

Dies unterteilt sich in vier Abschnitte:

1. **Das Aktivieren der Aufzeichnung**

Voraussetzung hierfür ist ein aktivierter SSH-Zugang. Der Befehl lautet:

syno_hibernate_debug_tool --enable 10

Die 10 steht dabei für ein Zeit-Intervall. Jeder Prozess welcher eine Datei länger geöffnet hält als dieses Intervall wird protokolliert.

2. **Die DS ihre Arbeit tun lassen**

Jetzt geht's ans warten. Noch schnell sicherstellen dass Hibernation aktiviert ist und dann die DS in Ruhe lassen. Es ist wichtig, dass kein eigener Zugriff auf die DS erfolgt, da das Ergebnis sonst verfälscht werden kann. Am besten ist es daher, gleich das LAN-Kabel zu ziehen. Nach ein paar Stunden kann es dann weiter gehen.

3. **Das Log entnehmen**

Zunächst muss man sich in den DSM einloggen. Die Adresse der Webseite sollte ungefähr so aussehen:

http://192.168.1.49:5000/webman/index.cgi

Als nächstes muss diese Adresse geändert werden:

http://192.168.1.49:5000/webman/index.cgi?debug=1

Ein Download sollte nun starten. Die empfangene Datei kann anschließend ausgewertet werden.

4. **Das Log wieder abschalten**

Damit die DS nicht wild weiter protokolliert und sich selbst aus dem Hibernation holt, ist es wichtig diese Funktion nach Abschluss des Tests wieder zu deaktivieren.

Erneut müssen wir via SSH auf unsere DS zugreifen:

syno_hibernate_debug_tool –disable

Sollte jemand den letzten Schritt vergessen, wird das Log bis zum nächsten Neustart weiter geschrieben. Anschließend werden die Nachrichten stattdessen in den Linux-Speicher unter */var/log/messages* geschrieben, was diese Datei daraufhin unbrauchbar machen würde.

2.26 „Piepton-Steuerung“

Diese etwas spaßig übersetzte Option findet sich interessanterweise unter „Energie“. Der Umfang ist je nach DiskStation unterschiedlich, da nicht jede Hardware eine Steuerung dieser Warntöne zulässt. Häufig zu finden sind u.a.: Piepton bei Gebläsestörung, Pieption bei Volume-Absturz, Pieption beim Hoch- und Herunterfahren …

2.27 DSM Update

Ein Update der Firmware ist sehr einfach. Man lädt die entsprechende Datei (Endung *.pat) bei Synology im Download Center[37] herunter, speichert sie auf dem Rechner (nicht der DS!) und öffnet in der Systemsteuerung „DSM Aktualisierung“.

Wer möchte, kann dort auch aktivieren, dass automatisch nach Updates gesucht werden soll. Wird eines gefunden, so wird man benachrichtigt und kann die Installation automatisch erfolgen lassen. Beta-Software wird über diesen Kanal jedoch nicht verbreitet. Wer also aktuellste Technologie testen möchte, sollte regelmäßig bei Synology oder der deutschen Community vorbeischauen.

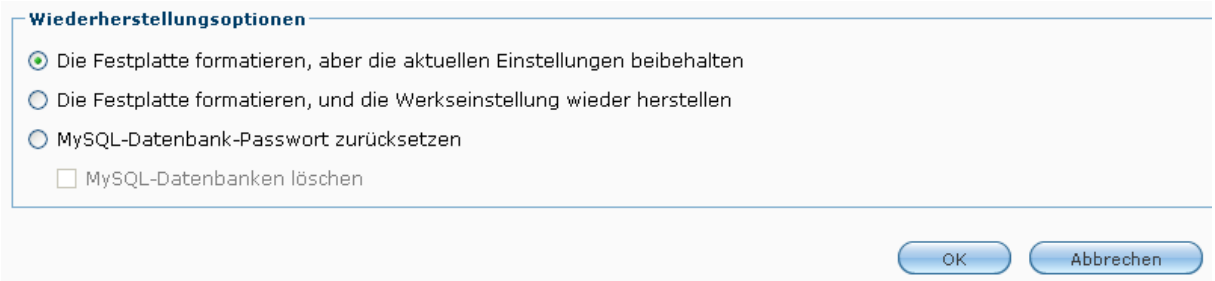
Wichtig: Ein Downgrade ist in einigen Fällen zwar mittels Modding möglich (entgegen der Aussage der Systemsteuerung, siehe deutsches Wiki[38]), doch dies ist stets mit einem hohen Risiko für Daten, Hardware und Nerven verbunden.

2.28 Wenn nichts mehr geht: Reset

Sollten Sie ihre DS einmal komplett „verkonfiguriert“ haben, hilft meist nur noch ein Reset. Davon gibt es drei Arten welche ich hier alle beschreiben möchte mitsamt ihren Konsequenzen.

2.28.1 Weboberfläche „Standard wiederherstellen“

Die erste Methode ist über die Weboberfläche erreichbar. Dabei werden die Festplatten formatiert. Ob auch das Betriebssystem zurückgesetzt werden soll, können Sie bestimmen. Dabei werden jedoch nicht die Partitionen gelöscht. Wenn es also Probleme mit dem Speichern von Daten oder ähnlichem gibt, dann ist dieses Reset ungenügend. Dabei werden die Volumen gelöscht und die Einstellungen auf den Zustand zurückgesetzt wie es direkt nach der Installation der Fall ist (wenn Sie möchten). Auch das MySQL-Passwort kann hier zurückgesetzt werden. Und wenn auch die Datenbanken weichen müssen, gibt es auch für diese eine entsprechende Option.



[37] http://www.synology.com/support/download.php?lang=enu
[38] http://www.synology-wiki.de/index.php/Downgrade_der_Synology-Firmware

2.28.2 Hardware 1: Passwort und Netzwerkeinstellungen löschen

An der Rückseite des NAS befindet sich ein kleines Loch wie es auch bei anderen Geräten üblich ist. Am einfachsten lässt sich der dahinterliegende Schalter mit einer Büroklammer betätigen. Halten Sie den Knopf dann für ungefähr 4 Sekunden bis das System **einen** Signalton ausgibt.

Dabei werden folgende Einstellungen zurückgesetzt:

- Admin-Passwort wird „“ sein (ohne Anführungszeichen, also komplett leer)
- Gast-Account wird deaktiviert
- DHCP wird eingeschaltet um Probleme mit der IP-Adresse zu beheben
- Jumboframes werden deaktiviert
- Port der Weboberfläche wird auf 5000/5001 zurückgesetzt
- PPPoE wird deaktiviert
- Link Aggregation wird deaktiviert
- Firewall wird deaktiviert

Damit sollten alle Netzwerkprobleme behoben sein und auch ein vergessenes Passwort ist jetzt kein Problem mehr. Doch dies zeigt auch: Seien Sie vorsichtig, wer Zugang zu Ihrer DS bekommt, also nicht virtuell sondern vollkommen real und sei es mit dem Schlüssel zum Schrank. Denn über den Reset kann das Passwort zurückgesetzt werden …

2.28.3 Hardware 2: Firmware löschen

Bei dieser Methode wird nun das gesamte Betriebssystem gelöscht. Doch zunächst zum Vorgehen: Drücken Sie die Resettaste bis zum ersten Signalton nach rund 4 Sekunden und lassen Sie ihn dann wieder los. Drücken Sie ihn erneut bis drei weitere Signaltöne ausgegeben wurden. Dann kann der Assistant wieder mit der Installation beauftragt werden. Die Daten welche auf den Volumen waren sollten nicht beschädigt worden sein. Doch: Backup ist immer Vorsicht. Murphys Gesetz sagt nun mal das alles schief gehen kann was nur geht …

Doch durch die Neuinstallation geht auch einiges neben den Einstellungen verloren, wie etwa:

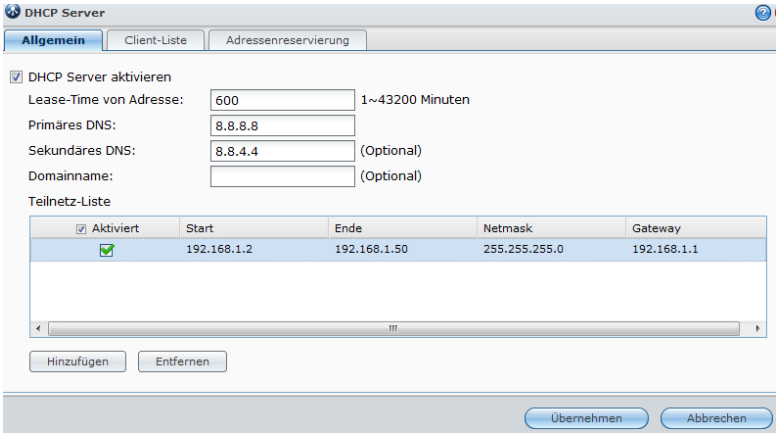
- Der Index für die Mediendienste muss neu erstellt werden, ebenso wie die Vorschaubilder für die Photo Station
- Alle Datenbanken gehen verloren
- Sämtliche Inhalte der Photo Station (wie Blogeinträge) sowie die Playlisten des iTunes-Servers gehen verloren
- Die Daten der Surveillance Station lassen sich mit Bordmitteln nicht mehr abrufen

Ein „Downgrade“ der Firmware, also ein herabsetzen auf eine ältere Version, ist auch so nicht möglich. Dazu gibt es eine – sehr heikle – Anleitung im Wiki.

3. Erweiterte Funktionen

3 Erweiterte Funktionen für komplexe Aufgaben und Netzwerke

3.1 DHCP-Server



In vielen Heimnetzen stellt der Router auch einen DHCP-Server zur Verfügung (mehr zur Theorie in Kapitel 1.4.3). In größeren Netzwerken kann man jedoch flexibler mit Adressen umgehen. Zusätzlich unterstützt der von Synology verbaute DHCP-Server auch anhand der MAC-Adresse fest zugeordnete IPs. Auch können unter „Client-Liste“ alle aktuell vergebenen Adressen eingesehen werden. Das oben genannte Kapitel zu DHCP sowie Kapitel 1.4.1 über IPv4 sollte man unbedingt gelesen und verstanden haben!

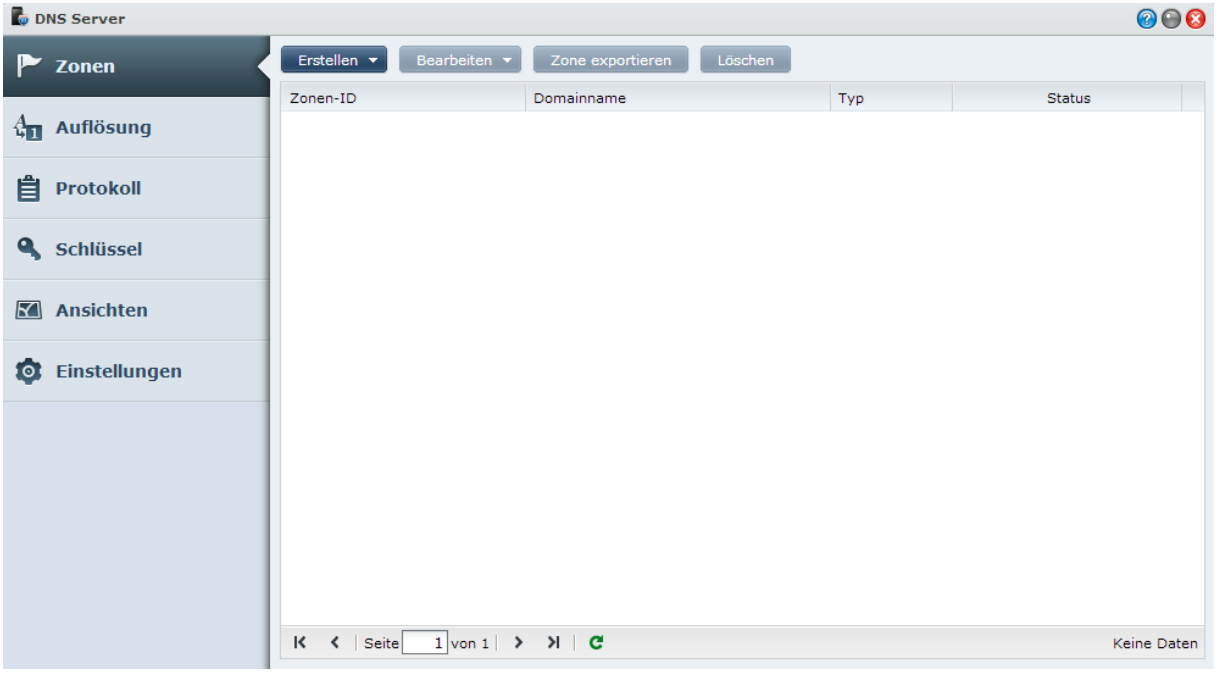
Kurze Ausfüllhilfe: Die „Lease Time“ bezeichnet, wie lange eine IP einer bestimmten MAC zugeordnet wird. Solange dieses Lease läuft, erhält ein Client stets dieselbe IP als Antwort vom DHCP. Die Angabe erfolgt in Minuten. Mit primärem und sekundärem DNS sind die sind im Netz vorhandene DNS-Server gemeint. Sind keine vorhanden, stellt der Internet-Provider (ISP) welche bereit. Häufig bietet auch ein Heimrouter einen DNS, welcher aber auch wiederum nur den Provider befragt. Es gibt aber auch offene Server, beispielsweise von Google[39].

Um Adressbereiche zu vergeben, muss man zunächst über die Schaltfläche „Hinzufügen“ eine Zeile erstellen. Dort muss man dann die erste zu vergebende Adresse („Start“) und die letzte („Ende“) vermerken. Zusätzlich noch die „Netmask“ (Stichwort Subnetzmaske und Netzwerkanteil) sowie das Gateway, also den Router angeben. Start und Ende müssen dabei innerhalb eines Netzes liegen. Der Netzwerkanteil darf sich daher nicht unterscheiden.

3.2 DNS-Server

Wie in Kapitel 1.7.1 beschrieben, ordnet DNS einer Domain die passende IP zu, und umgekehrt. Falls Sie mit „Reverse“ und „Forward“ im Zusammenhang mit DNS noch nichts verbinden, ist eine Lektüre von eben jenem Kapitel sehr ratsam.

[39] Die beiden IP-Adressen des Google-DNS sind 8.8.8.8 und 8.8.4.4
Leider haben Provider heutzutage gern die Angewohnheit, Seitenaufrufe für inkorrekte oder nicht vorhandene Seiten auf die eigenen, mit Werbung gepflasterten Suchseiten umzubiegen. Dies ist entgegen die gültigen Standards. Daher lohnen sich alternative DNS-Server durchaus.



Der DNS-Server begrüßt den Administrator beim ersten Öffnen mit einer ziemlich leeren Seite die es zu füllen gilt.

Die linke Seite birgt folgende Optionen:

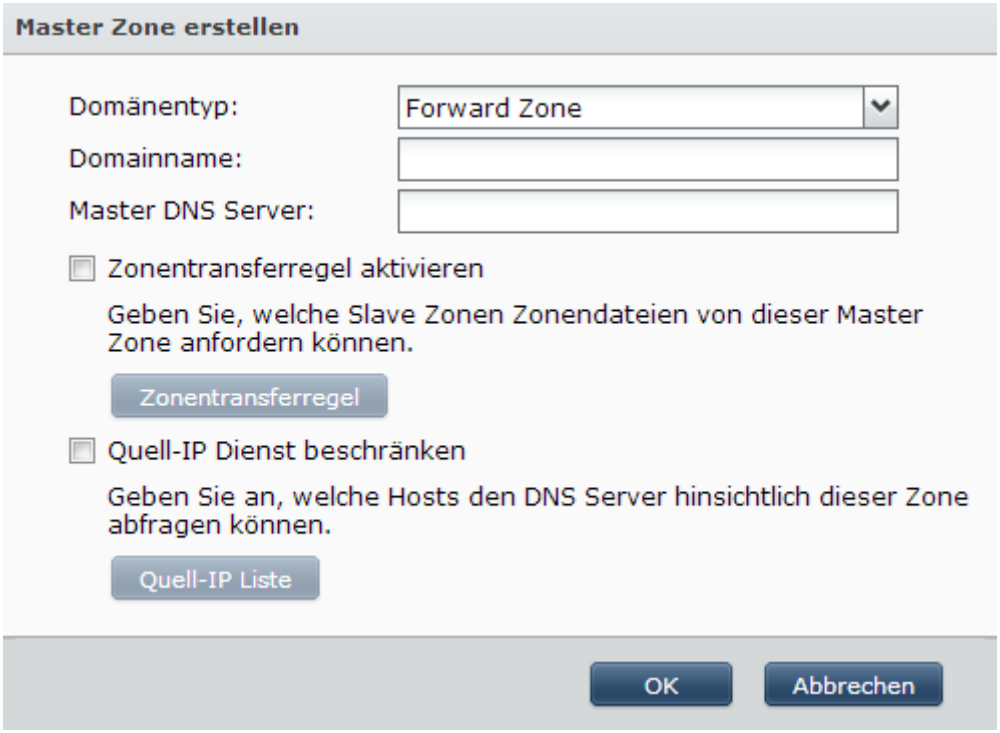
- **Zonen** – Hier lassen sich primäre und sekundäre Zonen anlegen und verwalten.
- **Auflösung** – Hier können DNS-Server für rekursive Anfragen benannt werden.
- **Protokoll** – Sammelt alles was an administrativen Änderungen durchgeführt wurde.
- **Schlüssel** – Zur Absicherung können TSIG-Schlüssel verwendet und generiert werden.
- **Ansichten** – Besser bekannt als „Split Horizon DNS“ können hier unterschiedliche Antworten an unterschiedliche Clients ausgeliefert werden.

„Zonen“, „Auflösung“ und „Schlüssel“ werden jetzt näher erläutert.

3.2.1 Zonen erstellen

Hier läuft die grundlegendste Konfiguration des DNS-Servers ab, wenn man selbst Domains verwalten möchte. Soll der DNS-Server aber nur Anfragen rekursiv bearbeiten (vergleichbar mit den DNS-Servern in vielen Heimroutern), ist eigentlich nur die Seite „Auflösung“ wirklich wichtig.

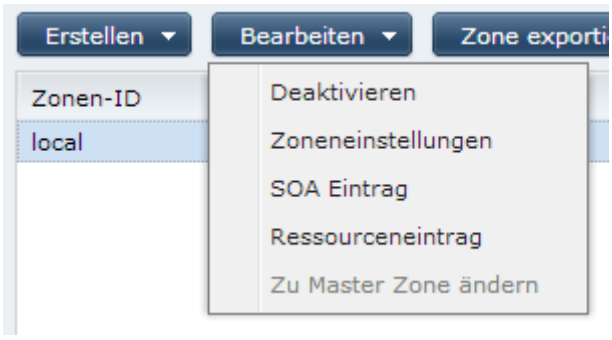
Über „Erstellen“ lässt sich auch eine bereits vorhandene Zonendatei einbinden. Die „händische“ Administration dürfte aber üblicher sein, es sei denn man migriert den Server.



Zunächst möchte der DNS-Server wissen, ob es sich um eine „Forward“ oder „Reverse“-Zone handelt, siehe auch den Theorie-Teil. Wird – wie hier – eine Master Zone angelegt, muss man die IP der DS unter „Master DNS Server“ eintragen. Bei einem Slave-Eintrag den DNS welcher als Master fungiert. Wenn mit Slave-Servern gearbeitet wird, ist es auch ratsam „Zonentransferregeln“ einzurichten, damit nicht jeder diese Daten wie ein Slave abrufen kann. Der Abruf vollständiger Zonendaten kann ein Sicherheitsrisiko darstellen und sollte somit entsprechend begrenzt bleiben. Über eine Quell-IP lassen sich schließlich noch die Clients einschränken. Wenn der DNS auch über das Internet genutzt wird, macht es u.a. Sinn interne Domains für solche Zugriffe zu sperren – um mal ein kurzes Beispiel anzuführen.

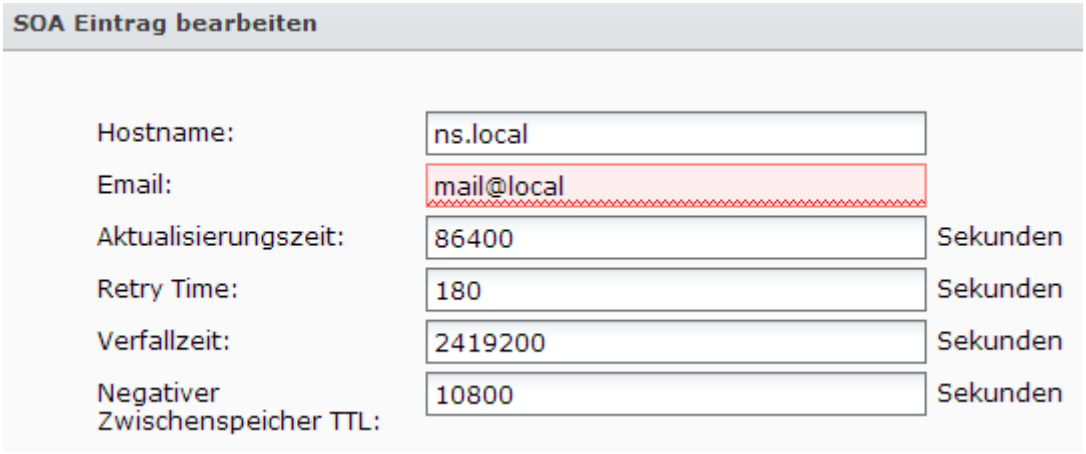
3.2.2 Zonen bearbeiten

Um nun richtige Einträge zu erzeugen, muss man die erstellte Zone wieder bearbeiten.



Momentan nicht mehr benötigte Zonen lassen sich dort deaktivieren. Man muss also mühsam erstellte Zonen nicht gleich löschen wenn man sie testweise nicht nutzen möchte. Unter „Zoneneinstellungen bearbeiten“ befinden sich die bereits aus „3.2.1 Zonen erstellen“ bekannten Optionen.

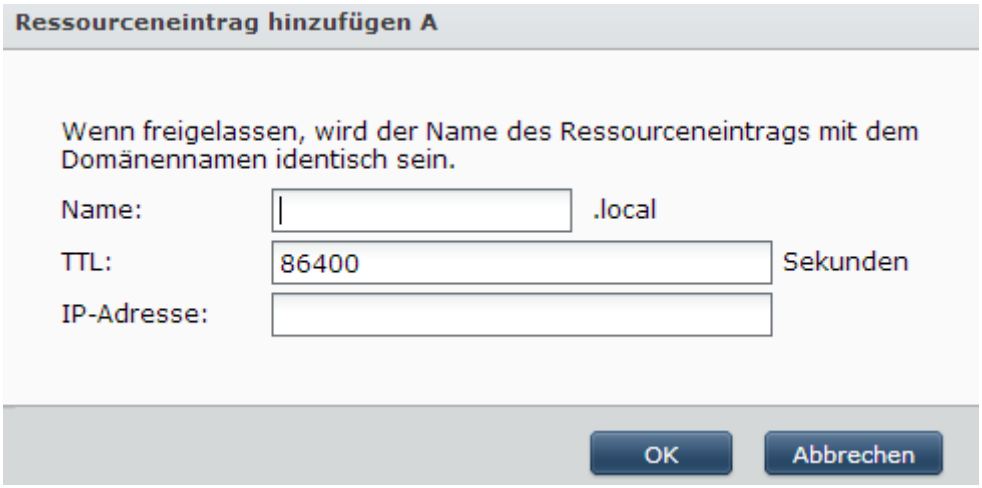
Unter „SOA Eintrag“ wird es jetzt wieder spannend.



„SOA“ bedeutet „Start of Authority“ und enthält viele wichtige Angaben zum Zonentransfer zwischen Zonen-Master und Slave. Synology hält sich dabei an die empfohlenen Werte.[40] Wichtig sind hier neben der obligatorischen E-Mail-Adresse:

- die „Aktualisierungszeit“ (Sekunden bis ein Slave die Zonendatei erneut abfragt und auf Änderungen prüft, Standard 24h),
- die „Retry Time“ (Sekunden bis ein Slave erneut abfragt, sollte der Master nicht geantwortet haben, Standard 2h),
- die „Verfallzeit“ (Sekunden von der letzten erfolgreichen Abfrage eines Masters bis zur Deaktivierung der Zone durch den Slave, Standard 1000h), und
- „Negativer Zwischenspeicher TTL“ (Sekunden bis ein Slave erneut beim Master nachfragt ob die von einem Client abgefragte Zone tatsächlich nicht existiert, Standard 2d).

Aber bisher ist noch nicht ein Gerät per DNS zusätzlich erreichbar. Dafür müssen nun „Ressourceneinträge“ angelegt werden. Die wichtigsten der verschiedenen Typen werden im Theorieteil erklärt. In der Praxis kommen am häufigsten „A“ (IPv4-Adresse) und „AAAA“ (IPv6-Adresse) zum Einsatz. Der Dialog im DNS-Server ist denkbar simpel:

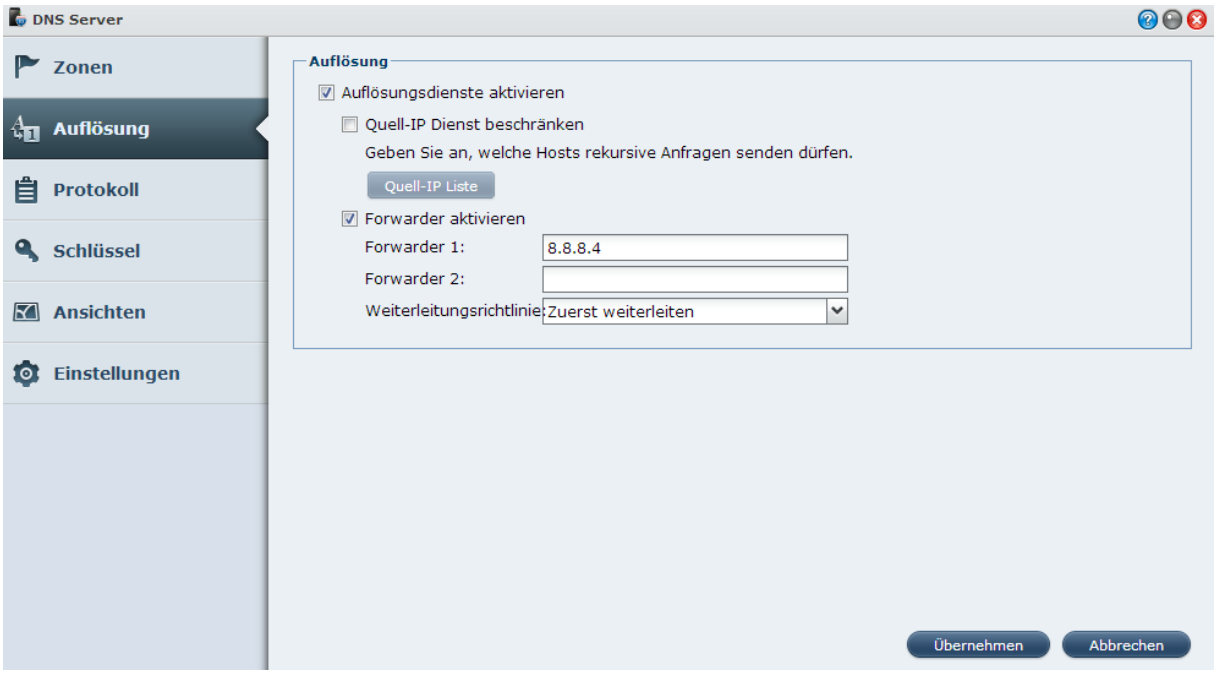


Benötigt werden nur der Name des Hosts (die Zone wird dahinter bereits angezeigt), die TTL („Time to Live“) und die zuzuordnende IP-Adresse.

[40] Siehe RIPE-203: http://www.ripe.net/ripe/docs/ripe-203, abgerufen am 21.2.2013, 18:35

3.2.3 Auflösung

An dieser Stelle kommt wieder die Theorie zum Einsatz.



Wie von dort bekannt, passiert es häufig dass der DNS-Server zunächst andere DNS-Server befragen muss um korrekt antworten zu können. Genau dieses Verhalten kann man hier konfigurieren. Der „Auflösungsdienst“ veranlasst den DNS-Server, iterative Anfragen zu stellen wenn er selbst keine passende Zone administriert.

Der DNS-Server kann dabei auf zwei Arten arbeiten: Entweder er fragt ausschließlich einen öffentlichen DNS-Server ab, oder er arbeitet sich selbst durch die gesamte DNS-Hierarchie bis zum gewünschten Ergebnis. Es dürfte leicht zu sehen sein, dass eine Anfrage an einen öffentlichen DNS-Server schneller ist als viele Anfragen an verschiedene Server. Allerdings liefern diese öffentlichen Server (bei Synology „Forwarder“ genannt) nur nicht-autoritative Antworten zurück. Man sollte dem Betreiber also schon ein Stück Vertrauen entgegen bringen. Entscheidet man sich dennoch für die schnellere Variante, muss man die „Forwarder“ entsprechend aktivieren und zwei IP-Adressen hinterlegen. Es gibt eine ganze Reihe von öffentlichen DNS-Servern die man nutzen kann. Jeder ISP betreibt außerdem eigene. Die halten sich aber häufig nicht an Standards und blenden Suchseiten mit Werbung ein statt die korrekte Antwort zu geben dass die Adresse nicht existiert. Das kann bei manchen Anwendungen schon mal zu Problemen führen. Besser ist es, Anbieter ohne solche Ambitionen zu wählen. Zum Beispiel betreibt Google zwei öffentliche Server, 8.8.8.8 und 8.8.4.4[41]

Sind die beiden aufgeführten Server dennoch nicht erreichbar, kann der DSM-Server entweder den Vorgang ganz abbrechen („Rootserver nicht abfragen“), oder den offiziellen Weg gehen und die autoritativen Server befragen („Zuerst weiterleiten“).

[41] Siehe auch: https://developers.google.com/speed/public-dns/, abgerufen am 21.2.2013, 18:06 Uhr.

3.2.4 Schlüssel

Um die Synchronisierung von Master- und Slave-DNS-Servern weiter zu sichern, kann mit Schlüsseln eine weitere Authentifizierung eingesetzt werden (neben der bereits genannten IP-Whitelist[42]).

Kennt ein Client also den Schlüssel („Schlüssel exportieren“), kann es mit diesem arbeiten. Das Erstellen eines Schlüssels ist sehr einfach. Beim Slave-Server muss dieser Schlüssel dann importiert werden. Es ist aber sehr wichtig, die Schlüssel gut zu sichern! Verschafft sich jemand Zugang zu diesem, kann er die Zonendateien abrufen. Das heißt: Zugang zur DNS-Server-Administration und insbesondere auch via SSH soweit einschränken wie möglich!

3.3 Syslog

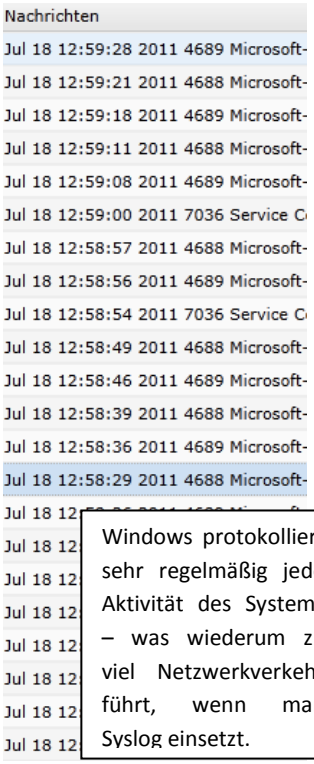
In komplexen Netzwerken, insbesondere in Firmen, sind Protokolle über etwaige Fehlermeldungen wichtige Indizien um Softwarefehler finden und Hardwarefehler vorbeugend erkennen zu können. Wenn man diese Meldungen daher zentral speichern, ansehen und analysieren kann, hat man ein gutes Werkzeug in der Hand um auftretende Probleme auch langfristig zu diagnostizieren. Synology stellt dazu einen Syslog-Server als Paket bereit. Die Option „Syslog“ in der Systemsteuerung des DSM stellt nur den Client zur Verfügung.

Der Server selbst ist schnell installiert und eingerichtet. Die Einstellungen sind recht simpel und schnell gemacht, sofern man weiß was man machen möchte:

- **Speicherort** – gibt den Gemeinsamen Ordner an, in dem sämtliche Daten gespeichert werden.
- **Transferprotokoll** – spezifiziert die Art der Übertragung (siehe unten).
- **Anschluss** – gibt den Port an, auf welchem der Syslog-Server auf Nachrichten wartet.
- **Protokolldrehung** – definiert, wie lange die Aufzeichnungen gespeichert werden.
- **E-Mail-Benachrichtigung** – veranlasst bei bestimmten Stufen den Versand einer E-Mail um kritische Probleme sofort zu melden
- **Sicheren Transfer aktivieren** – aktiviert bei TCP-Übertragungen eine Verschlüsselung der Nachrichten. Dies ist wichtig, wenn aus besonderen Gründen auch sicherheitsrelevante Informationen übertragen werden.

[42] Eine Whitelist listet alle erlaubten IP-Adressen (oder z.B. bei Antivirenprogrammen die erlaubten Dateien). Im Gegensatz dazu enthält eine Blacklist nur was verboten ist.

Um den Speicherbedarf ein wenig einzuordnen: Die zuständige Datei („SYNOSYSLOGDB“) wuchs in kurzen Tests in einer gemischten Windows-Linux-Umgebung auf etwa 1MB je 1000 Einträge.



Windows protokolliert sehr regelmäßig jede Aktivität des Systems – was wiederum zu viel Netzwerkverkehr führt, wenn man Syslog einsetzt.

3.3.1 TCP und UDP bei Syslog

Gut überlegt sollte aber die Auswahl zwischen UDP und TCP sein. Eine technische Auseinandersetzung mit beiden Methoden findet sich in Kapitel 1.5.1. Doch welche Auswirkungen hat dies auf den Betrieb eines Syslog-Dienstes?

Bei TCP ist garantiert, dass jede Nachricht ihr Ziel erreicht, denn der Server muss den Empfang bestätigen. Jetzt werden die meisten erst einmal sagen, „Perfekt, so soll es doch sein“. Aber die Probleme lauern im Detail: Mit diesem Verfahren gehen mehr Netzwerktransfer und mehr Rechenaufwand für Server und Client einher. Eine einzelne dieser Nachrichten mag für beide kein Problem sein, doch ein Syslog-Server muss dutzende, wenn nicht gar hunderte von Clients anbinden. Bedenkt man, dass Windows zum Beispiel jeden gestarteten Prozess (und seien es Hintergrunddienste die nur anlaufen wenn sie gebraucht werden) als Sicherheitsinformation protokolliert und damit gern ein paar Hundert Meldungen pro Stunde produziert, ergibt sich hier ein ernsthaftes Problem. Im schlimmsten Fall ist der Server überlastet, verweigert weitere Meldungen und stellt auch andere Dienste ein. Häufig hilft dann nur noch ein Neustart des gesamten Systems – verbunden mit der entsprechenden Downtime[43].

Deutlich anspruchsloser ist da UDP. Es versendet das Paket und hat damit seinen Dienst getan. Keine Bestätigung, keine Überprüfung. Ist der Server nah an der Grenze, verweigert er die Annahme und kann kurz Luft holen. Dafür können aber kritische Meldungen verloren gehen und Fehler werden nicht oder zu spät bemerkt.

Was jetzt fast schon klingt wie ein Plädoyer für UDP, hat einen entscheidenden Nachteil: Aufgrund seiner Einschränkungen kann UDP keinerlei Sicherheitsmechanismen integrieren. TCP hingegen ermöglicht eine Verschlüsselung über ein Zertifikat, welches auf Wunsch heruntergeladen werden kann („CA exportieren“ in den Einstellungen des Syslog-Server).

3.3.2 Sicherheitsstufen und die Nadel im Heuhaufen

Syslog ist „eigentlich“ ein durch zwei RFC-Papiere definiertes Verfahren (3164[44] und 3195[45]). Doch wie üblich wird sich über diese Festlegungen auch gern hinweggesetzt, etwa um eigene Erweiterungen zu verbauen (TCP in Syslog gehört zu diesen nicht spezifizierten, aber weithin genutzten Zusätzen). Entsprechend uneinheitlich ist in einigen Systemen die Verwendung der Sicherheitsstufen. 8 dieser Stufen klassifizieren die Nachricht von „beinahe überflüssig“ bis zum

[43] So bezeichnet man einen Zeitraum, in dem die Dienste eines Servers nicht erreichbar sind. Professionelle Hoster geben eine garantierte, maximale Downtime an. Wird diese überschritten, kann der Kunde sein Geld je nach Vertrag ganz oder teilweise zurück verlangen. Entsprechend kostspielig ist eine Downtime. Selbst wenn man nicht dafür bezahlt wird, ist ein nicht erreichbarer Server meist eine große Einschränkung an der Arbeit und kann ganze Abteilungen für gewisse Zeit Arbeitslos machen, weil notwendige Dokumente oder Anwendungen nicht zugänglich sind.

[44] http://tools.ietf.org/html/rfc3164

[45] http://tools.ietf.org/html/rfc3195

„Stufe-Rot-Notfall“. Der Synology Syslog-Server hinterlegt diese Stufe in der Ansicht mit passenden farblichen Markierungen um wichtiges schnell zu trennen.

Möchte man daher wirklich wichtige Meldungen finden, ist ein gut funktionierendes Filtersystem unerlässlich. Die „Suche“ des Syslog-Servers von Synology mag nicht zu den besonders detaillierten gehören, ist aber sehr einfach zu bedienen und bietet alles was man für erste Analysen benötigt.

Besonders wichtig für den Anfang ist die Eingrenzung der zahlreichen Meldungen über den „Hostname“, also den eindeutigen Namen des Geräts, sowie die „Stufe“. Hat man erste Anhaltspunkte, kann auch „Kategorie“ hilfreich sein. Sucht man etwa nach schwerwiegenden Fehlern, so hilft es die oberen Stufen nacheinander durchzusehen.

3.3.3 Die DS als Syslog-Client

Eine Disk Station kann aber auch einen Syslog-Server mit Daten speisen. In der Systemsteuerung des DSM unter „Syslog“ befindet sich dieser Client.

3.3.4 Einrichten der Clients unter Linux und Windows

Linux-Nutzer dürfen sich jetzt freuen: Syslog stammt aus dem Unix-Umfeld und ist daher mit einem der beliebten Programme wie syslog-ng auf den meisten Linux-Maschinen bereits vorinstalliert. Auch lokal verwenden Linux-Systeme diese Anwendungen um die Protokolle der verschiedenen Anwendungen zu sammeln. Dementsprechend ist die Konfiguration relativ einfach. Wie für Linux üblich wird die Konfiguration in Textdateien gespeichert. Auf den meisten Systemen läuft syslog-ng oder rsyslog. Auf dem von mir zum Testen verwendeten Linux Mint, das auf Ubuntu basiert, ist letzteres der Fall. Die Entwickler von rsyslog stellen freundlicherweise eine eigene Anleitung zur Verfügung.[46] Im Grunde muss man die Konfigurationsdatei um folgende Zeile erweitern:

```
*.*    @@other-server.example.net:514
```

Damit werden alle Meldungen entsprechend weitergeleitet. Wer nur gewisse Meldungen haben möchte, kann dies ebenso hier konfigurieren.

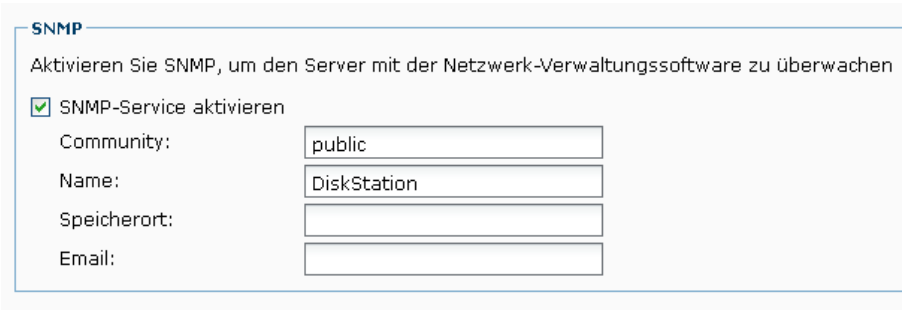
Windows hingegen hat eigene Gepflogenheiten um Ereignisse zu protokollieren. Versierte Nutzer kennen sie als „Ereignisanzeige“ (zu finden in der Systemsteuerung unter „Verwaltung“). Dort wird etwas anders gearbeitet als in Syslog, doch es gibt vielerlei Programme um auch Windows-Meldungen in diese Systeme einzubringen. Eine sehr gute und getestete Variante ist SNARE.[47] Es handelt sich dabei um ein OpenSource-Projekt, das von einer Firma vorangetrieben wird. Einmal installiert, bietet es administrativen Zugang über ein Webinterface. Eine Alternative zu dieser gibt es nicht, man sollte das Interface daher während der Installation aktivieren lassen! Standardmäßig hört dieses auf Port 6161 und kann so konfiguriert werden, dass es nur Verbindungen vom lokalen PC aus akzeptiert. Somit sollten Änderungen durch Außenstehende verhindert werden können. Zusätzliche Sicherheit verschafft das optionale Passwort.

[46] http://www.rsyslog.com/sending-messages-to-a-remote-syslog-server/
[47] Sourceforge-Seite des Projekts: http://sourceforge.net/projects/snare/
Alternative (Freeware): http://www.secureip.de/de/pro-ets.html

Zu Beginn müssen die Netzwerkeinstellungen um die IP des Syslog-Servers, sowie den Port ergänzt werden. Wichtig ist, dass SNARE nur TCP-Verbindungen aufbauen kann! Ein Betrieb des Syslog-Servers mittels UDP ist somit nicht möglich – andere Softwarealternativen bieten dies, haben jedoch an anderen Stellen Nachteile. Denn die große Stärke von SNARE ist die Filterfunktion mit welcher aus Windows-Meldungen RFC-konforme Mitteilungen werden. Im Webinterface verstecken sich diese hinter dem Begriff „Objectives Configuration“. Dort kann man viele Nachrichten unterbinden indem man „Information“ und „Success Audit“ entfernt. Somit werden nur Fehler gemeldet. Auf der anderen Seite fehlen damit auch Informationen die in einigen Szenarien, etwa einem Einbruch in das System bei bekanntem Passwort, welche nützlich für die Aufklärung sein können. Nur darf man anschließend nicht vergessen, die Änderungen auch an den Dienst zu melden: „Apply the Latest Audit Configuration“.

3.4 SNMP

SNMP dient zur Überwachung eines Netzwerks und ist insbesondere im gewerblichen Bereich sehr beliebt da es die einfache Administration eines gigantischen Netzwerks ermöglicht. Alle wichtigen Daten wie die Auslastung einzelner Rechner oder ganzer Serverfarmen lassen sich übersichtlich abrufen.



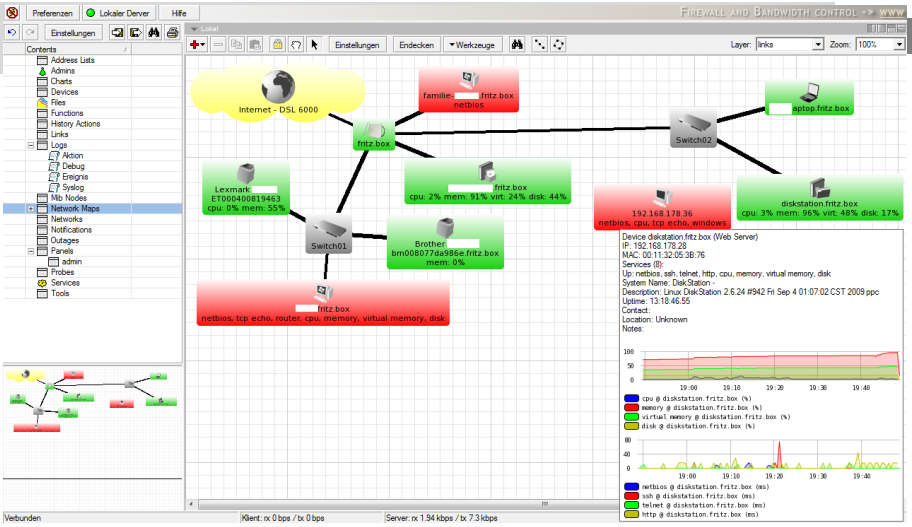
Auch eine DS unterstützt SNMP nach Aktivierung im DSM unter „Netzwerkdienste“. Die DS unterstützt SNMPv1 und 2. Diese ermöglichen keine Authentifizierung, somit sind diese Daten im Netzwerk für jeden zugänglich, der weiß was unter „Community“ eingetragen ist.

Speicherort und E-Mail dienen nur zur Identifizierung des Geräts in größeren Netzwerken, sind jedoch keinesfalls Pflicht.

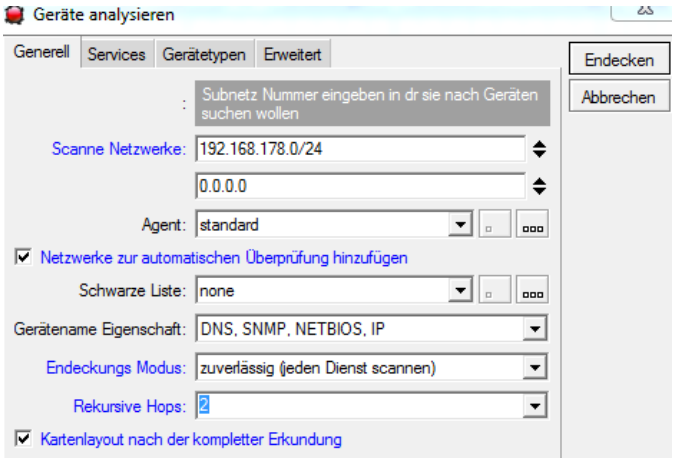
3.4.1 „The Dude“ – SNMP mit Server am praktischen Beispiel

Bleibt noch die Wahl einer passenden Gegenseite für den SNMP-Dienst. Je nach Vorlieben des Nutzers kann man unter einer Reihe von Share- und Freeware wählen. Recht einfach zu nutzen (im Verhältnis zu anderer Software) ist das kostenlose „The Dude“ von „MikroTik“,[48] da es nach wenig Zeit für Konfiguration schon brauchbare Ergebnisse liefert.

[48] http://www.mikrotik.com/thedude.php



Die Einrichtung erfordert meistens nur die Angabe des IP-Bereichs welcher in der Regel schon korrekt voreingestellt ist. Anschließend sucht „The Dude“ nach laufenden Geräten die sich hinter den IPs verstecken. Hat eine IP sich gemeldet, wird genauer abgesucht, darunter auch nach SNMP. Verweilt man nun eine Weile auf einem grünen Feld für das SNMP aktiv ist (meist erkennbar an Kurzinfos die unter der Netzwerkadresse stehen), so öffnet sich ein Fenster mit detaillierten Informationen und einer Verlaufsgrafik der überwachten Werte.



Wenn man nun die Übersichtlichkeit erhöhen will, kann man „Kabel“ verlegen und eigene Geräte (Switch) einfügen. Den Kabeln kann man außerdem eine Übertragungsgeschwindigkeit zuweisen, welche anschließend durch die Stärke der Linie verdeutlicht wird. Außerdem lassen sich noch viele weitere Dinge konfigurieren und Einfügen; die Möglichkeiten sind beinahe unbegrenzt.

Tauchen nicht sofort alle Geräte auf, sollte man zunächst sicherstellen dass sie eingeschalten und angeschlossen sind. Mit einem Klick auf „Endecken“ (das fehlende t ist falsch übersetzt) einen weiteren Suchlauf.

Wird „The Dude“ nicht gebraucht, minimiert es sich als kleine Fahne in den sogenannten System-Tray, also den Bereich neben der Uhr in Windows.

Das Drucken der entstandenen „Karte“ erfolgt am besten über die Funktion „Werkzeuge -> Exportieren“. Die entstandene Grafikdatei lässt sich ohne Umstände ausdrucken.

Und schon hat man immer einen Überblick über die Auslastung des eigenen Netzwerks.

3.5 LDAP / Directory Server

3.5.1 Verzeichnisdienste

Mit LDAP tritt jetzt ein weiterer Klotz in die Begriffswelt. Dienste wie dieser sind so alt, dass der Oberbegriff „Verzeichnisdienst“ sogar ins Deutsche übersetzt wurde. Bekannter als LDAP ist in dieser Familie wohl Active Directory (Microsoft) oder auch OpenDirectory (Apple). Mehr dazu gibt es wie üblich im ersten Kapitel.

In Verbindung mit einer DiskStation dient LDAP ausschließlich zur Authentifizierung von Benutzern.

3.5.2 Clients

Als Client für LDAP können ab Werk die meisten Unix-Abkömmlinge dienen. Mac OS und Linux werden von Synology als kompatibel angegeben. Windows hingegen geht mit ActiveDirectory (AD) einen eigenen Weg. Dies hat zur Folge, dass zusätzliche Software die Windows-Anmeldung an die Hand nehmen muss. Dazu eignet sich z.B. pGina.

3.5.3 DiskStations als Client

Doch natürlich hat Synology es sich nicht nehmen lassen, LDAP als vollständige Alternative zu Microsofts AD einzubinden. Direkt neben dem entsprechenden Knopf in der Systemsteuerung gibt es daher den LDAP-Client. Zur Konfiguration werden die Server-Adresse (DNS oder IP), die Art der Verschlüsselung und der Basis-DN, welcher vom Synology-Directory-Server nach Eingabe der Einstellungen angezeigt wird und sich aus dem FQDN zusammensetzt.

Über die Reiter kann zu den Benutzern und Gruppen gewechselt und die Berechtigungen vergeben werden. Es ist daher unbedingt notwendig zu wissen, welche Benutzer in Gruppen organisiert sind. Der Client hat des Weiteren nur lesend Zugang zu den verschiedenen Daten und die dort gemachten Einstellungen landen nicht im Server.

Bild: Unter (cc)-Lizenz von „Son of Groucho“ (Flickr)

4 Backup!

Über die Möglichkeit eines Raids wurde ja bereits gesprochen. Doch was wenn man versehentlich alles formatiert (löscht) und dabei auch die wichtigen Firmen-Unterlagen mit verloren gehen? Oder wenn ein Hacker eindringt und entsprechendes veranlasst? Und wenn einmal mehrere Festplatten gleichzeitig kaputt gehen (oder bevor man eine neue beschaffen konnte)? Genug der Albträume. Denn hier geht es um deren Lösung. Man sollte regelmäßig ein Backup auf eine externe Quelle durchführen. Dabei kann es sich um eine externe Festplatte genauso handeln wie ein weiteres NAS oder einen Server in der Cloud.

DIE SICHERUNG VON PCS UND ANDEREN ENDGERÄTEN WIRD HIER JEDOCH NICHT BEHANDELT.

4.1 Ein wenig Theorie

Auch bei diesem Thema kommt man auch hier nicht um ein wenig Theorie herum. Öffnet man auf Wikipedia die Seite zu Backup (dt. „Datensicherung“), so findet man unter „Sinn der Datensicherung“ den kurzen aber treffenden Satz:

„Die Datensicherung dient dem Schutz vor Datenverlust.“ [49]

So einfach kann man es auch ausdrücken. Nicht weit davon entfernt findet man ein weiteres wichtiges Kapitel: „Gesetzeslage“. Denn es ist in Deutschland für Unternehmen Pflicht, gewisse Daten regelmäßig zu sichern. Was sich für Nicht-BWL-studierte anhören mag wie weitere Geldverschwendung, hat einen ernsten Hintergrund. So schreibt das Gesetz Aufbewahrungsfristen für verschiedene Daten vor – von Rechnungen bis Grundbucheinträgen. Außerdem muss sichergestellt sein, dass diese Daten nicht verändert werden.

Doch eigentlich müsste man ein Backup nicht durch das Gesetz festschreiben. Sie sollte für jeden Anwender selbstverständlich sein. Ich gebe zu, ich trage schon wieder sehr dick auf. Aber auch wer sich seine DiskStation nicht zum Backup gekauft hat, könnte es nun zum Anlass nehmen sich ein paar Gedanken dazu zu machen.

Entscheidend für ein Backup sind die Kriterien der zeitlichen und örtlichen Trennung. In der Praxis bedeutet das: Kämpft man beispielsweise mit einer defekten oder durch einen Virus verunstalteten Datei, so muss das Backup schon etwas Zeit her sein falls man dies erst Tage oder Wochen nach der Veränderung bemerkt. Man sollte sich also gut überlegen, wie lange ein Backup gesichert bleibt und wann es gelöscht bzw. vernichtet (z.B. CD) wird. Dies hängt auch maßgeblich von der Sicherungsmethode ab, denn die Aufbewahrung von CDs und DVDs ist günstiger als eine fachgerechte Lagerung von Festplatten. Magnetbänder sind für große Mengen hingegen nach wie vor das Mittel der Wahl. Außerdem besagt die örtliche Trennung, dass man die USB-Festplatte nicht immer neben dem PC stehen haben sollte. Bei einer DiskStation kann eine dauerhaft angeschlossene USB-Festplatte beispielsweise bei einem Stromschlag beschädigt werden, was Originaldaten und Backup zugleich vernichtet. Ideal wäre daher die Speicherung in einem anderen Gebäude oder zumindest in einem anderen Gebäudeteil um bei Bränden die Backups retten zu können ohne selbst direkt in Gefahr zu sein.

[49] Quelle: http://de.wikipedia.org/wiki/Datensicherung, abgerufen am 24.06.2011, 23.20 Uhr

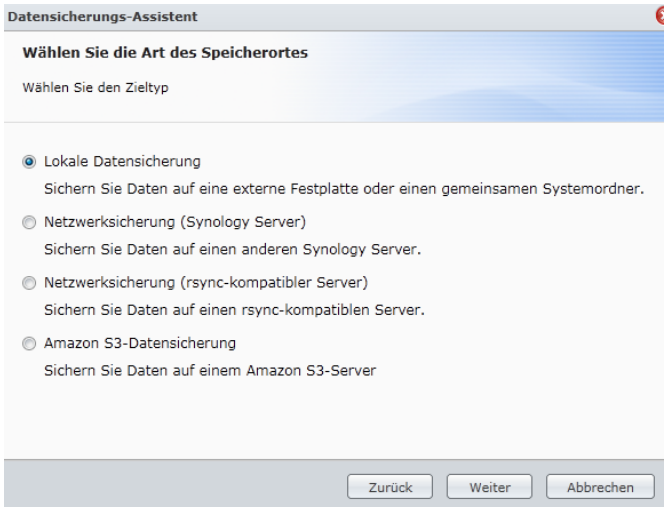
4.1.1 Murphys Gesetz

Murphys Gesetz ist keine Grundregel der IT. Sie stammt von einem Ingenieur mit dem Namen Murphy und beschreibt mehr eine Lebensweisheit. In der IT gewinnt sie aber eine ganz besondere Bedeutung. Die vereinfachte, umgangssprachliche Variante lautet: *„Alles, was schiefgehen kann, wird auch schiefgehen“.* Was bedeutet das in Bezug auf Backups? Wenn man auf ein solches zurückgreifen muss, wird auch das Backup selbst nicht mehr zu gebrauchen sein. Ein möglicher Fall wäre ein Problem während der Backuperstellung, durch das der gesamte Datensatz unbrauchbar, weil unvollständig oder korrupt, wird.

Hinter Murphys Gesetz verstecken sich unter anderem auch psychologische Aspekte. Es lehrt uns, dass ein einzelnes Backup nicht genügt. Versionierung, sowie ein Anfertigen weiterer Backups sind daher mehr als Zusatzaufgaben – es sind Notwendigkeiten in vielen Konstellationen.

4.1.2 Die Möglichkeiten

Um ein Synology NAS zu sichern, gibt es verschiedene Möglichkeiten.



- Externer Datenspeicher (USB/eSATA)

Die bekannteste Form des Backups sichert schlicht auf USB-Sticks, externe Festplatten und vergleichbare Systeme. Es zeichnet sich durch recht geringe Anschaffungskosten aus. Dafür haben solch externe Speicher aber auch die höchste Fehlerquote.

- rsync- und Synology-Server

Die DiskStations können auch untereinander Daten automatisiert austauschen. Da dies mittels dem Open Source-Programm „rsync“ geschieht, sind auch andere rsync-kompatible Speicher (meist Linux-Server oder andere NAS-Geräte) mit dieser Methode bestückbar. Hier kann mit sehr wenig Aufwand bei überschaubaren und kalkulierbaren Kosten eine sehr komfortable Lösung erzielt werden. Insbesondere wer mit den Daten auf seinem NAS Geld verdient, sollte dies ins Auge fassen.

- Online-/Cloud-Backup

Es gibt mittlerweile viele Anbieter welche Speicherplatz im Internet anbieten. Unter dem Schlagwort „Cloud“ hat auch diese Art von Dienst einen großen Schub erfahren und wird von vielen Benutzern eingesetzt. Als Backup kann ein solcher Speicher eine sinnvolle Erweiterung

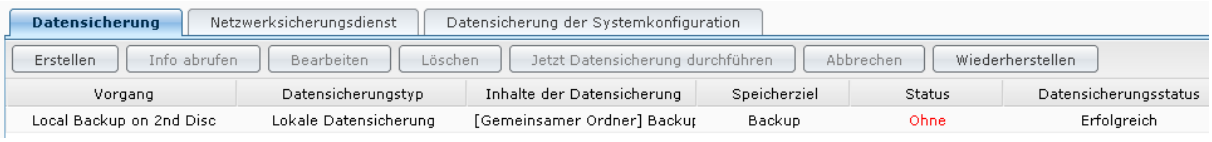
sein, denn die Verantwortung für die sichere Aufbewahrung wird so an einen Dienstleister übergeben. Doch auch rsync lässt sich bei vielen Anbietern ohne Aufpreis verwenden. Das vereinfacht häufig die Einrichtung.

4.2 Externe Festplatten-Sicherung

Die einfachste Möglichkeit die eigenen Daten zu schützen sind preiswerte, externe Festplatten. Diese können an freie USB-/eSATA-Schnittstellen gehängt werden. Zunächst sollten Sie sicherstellen, dass die neue Speichererweiterung auch erkannt wird. Eine anschließende Formatierung unter „Systemsteuerung“ -> „Externe Geräte“ ist nicht zwingend notwendig (externe Speicher werden meist vorformatiert geliefert), empfiehlt sich aber in den meisten Konstellationen.[50] Hier bleibt Ihnen die Wahl zwischen vier Dateisystemen. Zum einen dem Linux-typischen „ext3“, dessen Nachfolger „ext4“, dem Windows-Standard „FAT32“ und dem neueren „NTFS“ ebenfalls aus dem Hause Microsoft. Am Ende ist die Entscheidung einem selbst überlassen. Doch sollte man bedenken, dass Linux mit dem nativen Format, also ext3/ext4 schneller arbeiten kann und FAT32 darüber hinaus keine Dateien größer als 4 GB akzeptiert sowie keine Sonderzeichen als Dateinamen aufnehmen kann. Und NTFS ist unter Linux eh ein eigenes Kapitel mit vielen Unbekannten.

Ist die Formatierung abgeschlossen, öffnen Sie „Datensicherung und -wiederherstellung“. Nach einem Klick auf „Erstellen“ öffnet sich ein Fenster, welches eine Schritt-für-Schritt-Anleitung enthält. Dazu gehören die Auswahl der zu sichernden Ordner und anderes.

Problematisch ist hier häufig der Faktor Mensch: Um Schutz vor Diebstahl, Blitzschlag und mehr zu gewährleisten, muss der Datenträger nach erfolgtem Backup an einem anderen Ort aufbewahrt werden, was meist als lästig empfunden wird. Man sollte sich auch aus diesem Grund insbesondere bei externen Datenträgern über 2 Sicherungsziele Gedanken machen.



4.3 Netzwerksicherung

Wer noch eine zweite DiskStation besitzt, kann diese zur Sicherung der eigenen Daten verwenden. Doch diese Möglichkeit ist nicht auf Synology-Produkte beschränkt. Synology verwendet die offene „rsync“-Software zur Datensicherung, welches verschiedene Firmen nutzen/unterstützen. Auch selbstgebaute oder gehostete Linux-Server lassen sich meist problemlos mit rsync ausstatten.

Zunächst muss dieser Dienst wie alle anderen auf beiden DS aktiviert werden. Die entsprechende Option befindet sich unter „Sicherung -> Netzwerksicherungsdienst“. Anschließend richtet man die Sicherung unter „Sicherung -> Netzwerksicherung“ ein. Das Vorgehen ähnelt dabei dem der Sicherung auf eine externe Festplatte.

[50] Der Vollständigkeit halber: Bei einer Formatierung werden sämtliche Daten gelöscht (im genannten Fall also auf der externen Festplatte). Bei einem Backup-Medium ist eine Formatierung vor ab aber sehr empfehlenswert. Wer ganz sicher sein will, überschreibt das gesamte Medium vorab noch einmal. Dabei werden defekte Sektoren aussortiert.

Es werden nicht admin-Rechte auf die DiskStation oder den Server benötigt, auf die/den gesichert werden soll. Es reicht ein eingeschränkter Account mit Zugriff auf mindestens einen Ordner als Ziel für das Backup.

4.4 Online-/Cloud-Backup

Einmal bei Sicherungen über Netzwerke angekommen, kann man auch den Transfer über etwas weitere Strecken in Betracht ziehen. Mit den immer leistungsfähigeren Netzen der Internetprovider können auch größere Daten zu Rechenzentren übertragen werden. Die Angebote sind dabei sehr vielfältig. Bei einigen mietet man sich ein Stück „virtuelle Festplatte“ und bezahlt einen Festpreis, bei anderen wird akribisch nach Nutzung abgerechnet (etwa bei Amazon, welche auch Begriffe wie „Gigabyte pro Stunde“ pflegen und dazugehörige Werte berechnen). Je nach Art und Zweck des Backups kann man daher frei wählen und eine pauschale Empfehlung ist schlicht nicht möglich.

4.4.1 Amazon

Der Internetriese zählt auch in diesem Gebiet zu den größten Anbietern. Je nach den Anforderungen gibt es bei Amazon zwei Produkte zur Auswahl: Amazon S3 und Amazon Glacier.

An eines sollte man bei Amazon immer denken: Als Unternehmen mit Sitz in den USA gelten besondere Gesetze. Die Rechtslage zur Verwendung in Europa ist da etwas schwierig. Ohne Rückfrage mit einem Fachanwalt würde ich Unternehmen und Organisationen eine Lagerung der Daten bei Amazon – auch im europäischen (sprich Irischen) Rechenzentrum – nicht empfehlen. Für den persönlichen Gebrauch muss sich jeder selbst überlegen wem er seine Daten anvertraut.

S3 ist ein „einfacher“ Speicher auf den man nach Belieben zugreifen kann. Für gewisse Aktionen fallen bestimmte Gebühren an und man bezahlt penibel für den Zeitraum in dem man Speicher nutzt. Alles strikt nach Verbrauch. Amazon gehört damit nicht zu den „Flatrate“-Anbietern. Eine Datensicherung zu Amazon S3 lässt sich über die DSM-Applikation „Datensicherung und –wiederherstellung“ einrichten. Allerdings muss man sich ein wenig einarbeiten bis man versteht, was alles eingestellt werden muss und wie Amazon den Speicher verwaltet. Einmal konfiguriert verhält es sich aber wie jedes andere Backup.

Für Amazon Glacier gibt es ein zusätzliches Programm welches über das Paketzentrum angeboten wird. Glacier lockt mit deutlich günstigeren Preisen für die langfristige Speicherung. Allerdings muss man eine Wiederherstellung dann deutlich teurer bezahlen. Des Weiteren sind die genauen Kosten einer Wiederherstellung von der Geschwindigkeit des Datenabrufs abhängig.

Amazon eignet sich gut für ganz große Datenmengen, vor allem aufgrund der Preise.

Link: http://aws.amazon.com/s3/

4.4.2 Strato

Der wohl größte Anbieter einer „Online-Festplatte“ im deutschsprachigen Raum setzt dagegen auf einfach zu kontrollierende Kosten. Man entscheidet sich bei „HiDrive“ für eine bestimmte Größe und kann bis zu dieser Grenze Daten hoch- und herunterladen. Für Up- und Download sowie weitere Aktionen fallen keine Kosten an. Ein typischer „Flatrate“-Anbieter. Außerdem gibt es von Strato eine Applikation die man über das Paketzentrum beziehen kann. Der Nachteil des Geschäftsmodells ist aus Sicht des Kunden aber, dass man auch für Speicher zahlt den man unter Umständen nicht nutzt und daran häufig auch per Vertragslaufzeit gebunden ist.

Link: http://www.strato.de/online-speicher/

4.4.3 Rsync-Anbieter

Rsync ist ein sehr verbreitetes Protokoll zur Datensicherung in Netzwerken. Durch die effektive Verschlüsselung lässt es sich problemlos auch über das Internet hinweg einsetzen. An genau diesem Punkt setzen Anbieter an, die Speicherplatz bereitstellen auf den man (u.a.) mit rsync zugreifen kann. Eine Datensicherung ist dann über die Bordmittel des DSM schnell eingerichtet. Einige Anbieter können dabei die Platzhirsche preislich unterbieten.

Ein günstiger Anbieter aus dem deutschsprachigen Raum ist EUserv:

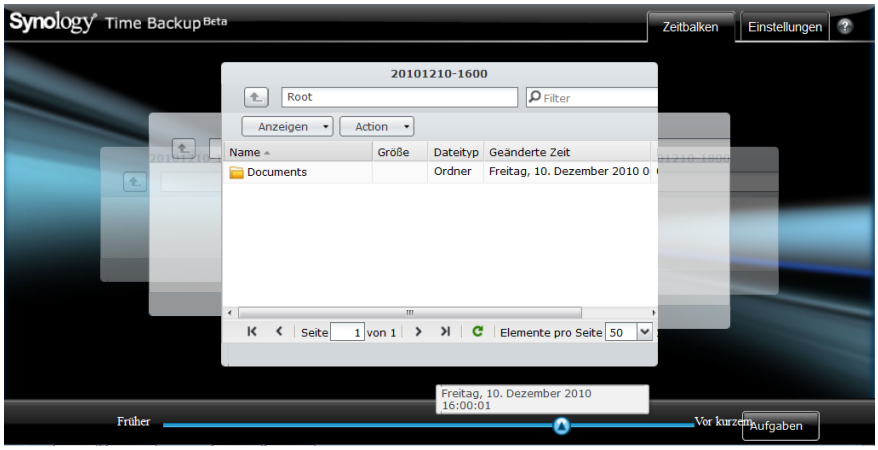
http://www.euserv.de/produkte/server/optionen/ftp-backup.php

4.5 Interne Sicherung

Eine interne Sicherung kopiert eigentlich nur die Daten auf ein angegebenes Ziel. Wer dieselbe Platte als Ziel verwendet, wird daher nur gegen unbeabsichtigtes Löschen abgesichert sein. Ein wirkliches Backup entsteht erst durch die Nutzung einer anderen Platte als Ziel. Und auch sonst ist diese Methode ziemlich unspektakulär und unsicher. Auch bei Blitzschlag etc. wären die Daten verloren.

4.6 Synology Time Backup

Ein wichtiger Aspekt bei Backups ist häufig auch die Sicherung verschiedener Versionen. Synology trägt mit der Anwendung „Time Backup“ dieser Anforderung Rechnung. Time Backup ist als zusätzliches Paket im Paketzentrum erhältlich. Es kann dabei genau festgelegt werden, in welchen Abständen Backups angelegt werden sollen. Um einen einfachen Einstieg zu ermöglichen, hat Synology aber auch bereits einen eigenen Sicherungsplan hinterlegt. Einzige Bedingung ist die Sicherung auf ein anderes Volumen oder eine andere DiskStation. Wenn die Daten also auf volume1 liegen, kann nicht auf selbiges gesichert werden.[51] Auch ist die Anzahl an Datensicherungen innerhalb von Time Backup je nach Prozessorgeschwindigkeit limitiert. Backups auf andere DiskStations sind sogar nur auf einigen Geräten möglich. Doch auch bei diesen Geräten sollte man nur wirklich wichtige Daten in kleinen Mengen mit Time Backup sichern; hier ist bereits häufig Kritik über geringe Performance bei sehr hoher Prozessorauslastung bekannt geworden.



4.7 Einstellungen

Bei eventuellem Reset des Gerätes ist es natürlich auch sehr hilfreich, wenn die Einstellungen sowie alle erstellten Benutzer(-Gruppen) mit gesichert sind. Bei einigen Datensicherungen lassen sich die Konfigurationen optional ins Backup integrieren .Man kann aber auch über den DSM eine spezielle Datei herunterladen. Die entsprechende Option findet sich unter „Datensicherung- und

[51] Wer ein Gerät mit nur einer Festplatte verwendet, kann mit einer Firmware ab DSM 3.1 auf einer Festplatte verschiedene Volumen anlegen mit jeweils unterschiedlicher Größe.

wiederherstellung -> Sichern der Systemkonfiguration“. Es empfiehlt sich außerdem, alle Protokolle in regelmäßigen Abständen zu sichern um im Notfall Problemen auf die Spur kommen zu können.

4.8 LDAP Server

Der Verzeichnisdienst der DS muss separat über dessen grafische Verwaltung gesichert werden. Zu beachten ist hier, dass der gesamte Dienst für die Zeit der Sicherung angehalten wird – man sollte also nicht am frühen Morgen einen Zeitplan einrichten, wenn gerade alle Benutzer sich versuchen anzumelden.

4.9 LUN-Backup

iSCSI-Speicherblöcke, sogenannte LUNs, lassen sich ebenfalls sichern, wahlweise auf einen Ordner oder ein Synology NAS im Netzwerk. Die Einrichtung entspricht weitestgehend dem bisher gesehenen, jedoch kann pro Aufgabe nur ein LUN gesichert werden.

4.10 Datenrettung

Doch auch die besten Strategien werden einmal auf ihre Belastbarkeit getestet. Wenn ein Dateisystem laut dem DSM zusammenbricht oder anderweitig Probleme macht, möchte man vor dem Experimentieren natürlich seine Daten im sicheren Wissen. Daher hier ein kleines Tutorial, wie man Dateien von einer intakten Festplatte retten kann, die **nicht in einem Raid oder JBOD betrieben wurde**. Denn das Problem liegt im verwendeten Dateisystem: Es kann mit Windows nicht ohne weiteres ausgelesen werden. (ext3/ext4)

Benötigt wird:

- Ein USB-SATA-Adapter ODER ein geöffneter PC mit interner SATA-Schnittstelle
- Eine leere CD und einen PC mit CD-Brenner inkl. Software
- Internetverbindung
- Die aus der DS gerettete Platte

Ich werde in meiner Anleitung unter den vielen verfügbaren Linux-Distributionen das beliebte „Ubuntu“ verwenden.

Den Download gibt es u.a. hier: http://wiki.ubuntuusers.de/Downloads

Ich habe den Torrent-Download auf meinen PC geladen. Herausgekommen ist eine .iso-Datei. Praktisch jede Brenn-Software kann ein solches Image auf eine leere CD/DVD brennen, auch ein USB-Stick lässt sich mit etwas mehr Arbeit verwenden.

Nun zur Hardware: Ich werde meine Festplatte über einen Adapter an einen USB-Anschluss klemmen. Wie bereits erwähnt, können Sie aber auch einfach eine interne SATA-Schnittstelle nutzen.

Passen Sie beim Anschließen auf die Pins auf.

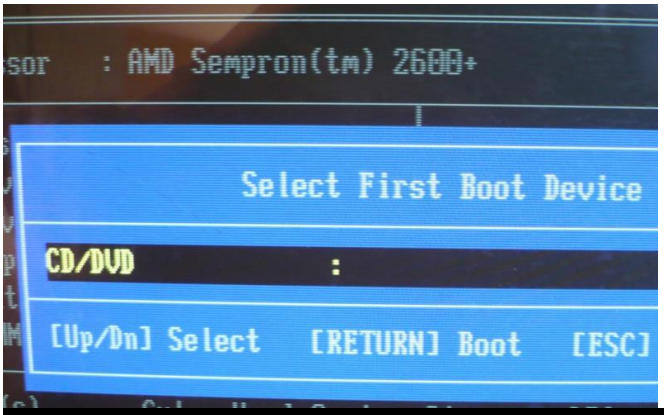
Beim USB-Adapter sollten Sie mit dem Anschließen aber warten, bis Linux gestartet ist. Doch nun zum Bootvorgang:

Die meisten PCs möchten zunächst von der Festplatte booten. Es gibt aber bei jedem

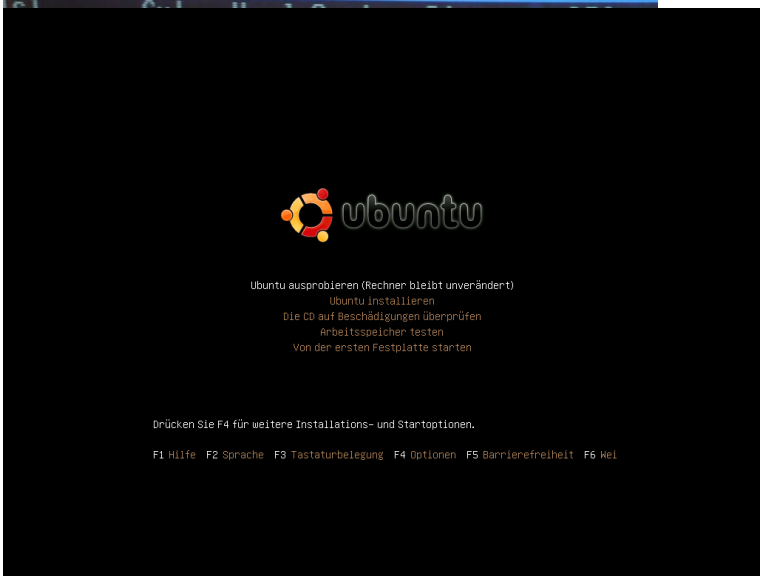
BIOS eine Taste, durch die man die Quelle selber wählen kann. Wenn Ihnen der Startbildschirm zu kurz ist, lässt sich die alte, aus DOS-Zeiten stammende „Pause“-Taste verwenden, um alles anzuhalten. Suchen Sie dann den Bildschirm nach dem Hinweis ab, drücken Sie erneut Pause und dann die entsprechende Taste. Bei meinem Beispiel mit AMI-BIOS ist das die F11-Taste.

Auf dem ersten Bild ist der Boot-Bildschirm zu sehen. Hier sind der Hersteller mit Symbol oben links, der Prozessor (zugegeben, mein Test-System ist ein bisschen veraltet) in Zeile vier und das Wichtigste für dieses Vorhaben: Die beiden Tasten F2 Für den BIOS-Setup und F11 für das Boot-Menü vermerkt. Ganz unten steht dann noch, dass ich keine Festplatte eingebaut habe. Wie gesagt: Es handelt sich um mein Test-System.

Nach besagter Taste F11 sollte ein paar Sekunden später ein Menü erscheinen, welches alle möglichen Boot-Geräte aufzählt. Ob das Booten dann auch wirklich klappen wird, ist eine andere Geschichte …



Das nächste Bild zeigt ganz oben noch einmal meinen Prozessor und darunter das geöffnete Menü. Da ich außer dem CD-Fach kein anderes Gerät eingebaut habe, welches sich zum Booten eignen würde, steht nur dieses zur Auswahl. Und da Ubuntu ja auf einer CD liegt, braucht man auch nicht mehr.



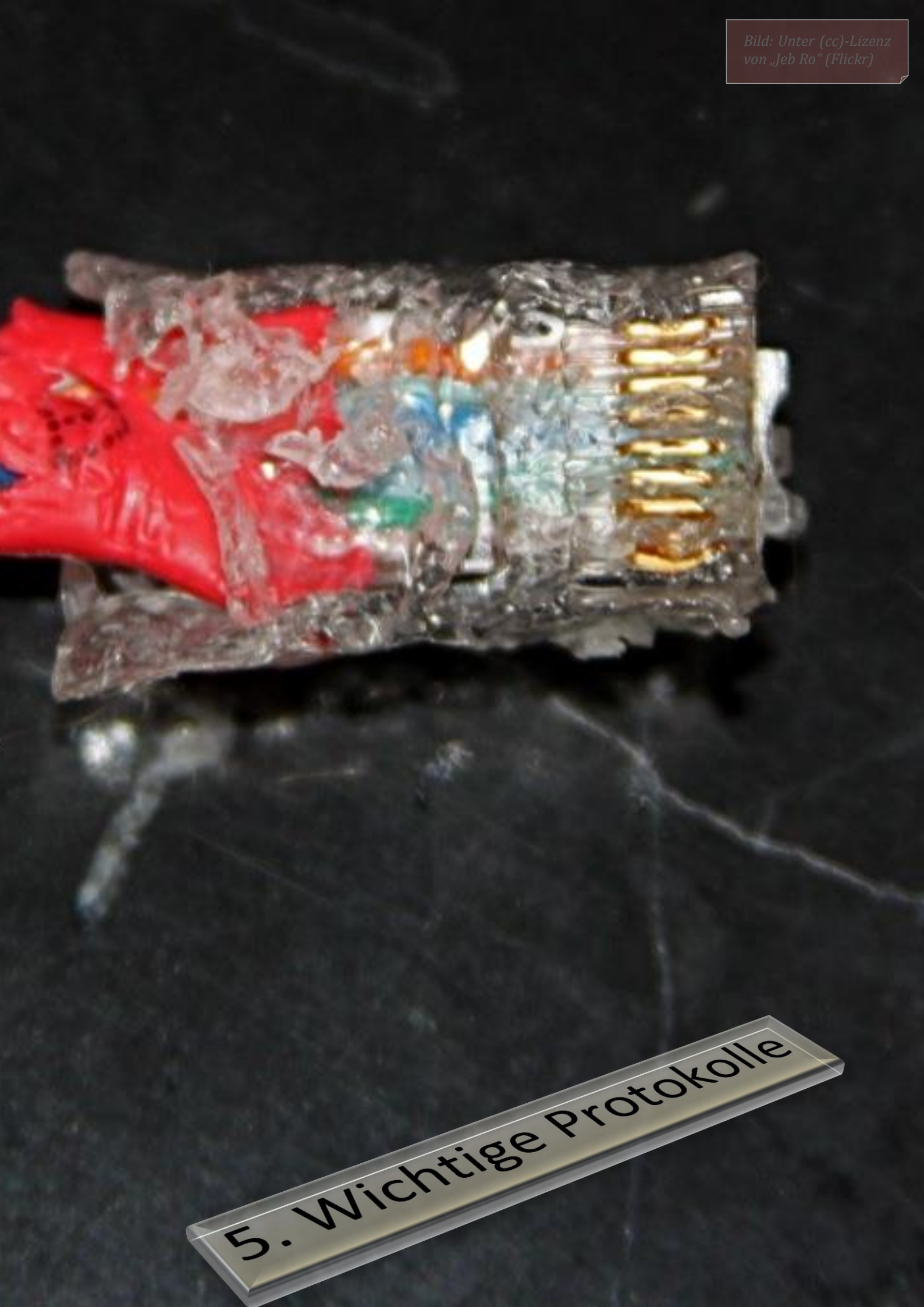
Dann sollte das BIOS kurz zeigen, dass es verstanden hat und schließlich die CD starten. Nach ein paar Sekunden meldet sich schließlich Ubuntu mit seinem Start-Bildschirm und fragt, ob es sich Starten, Installieren oder was auch immer soll. Hier ist aber nur die erste Option interessant. Noch schnell die Sprache überprüfen und dann kann Ubuntu starten. Noch ein letztes Mal warten (ruhig Geduld haben, denn hier muss ein komplettes System in den RAM kopiert werden) und dann kann es auf dem Desktop losgehen.

Ohne weitere Anmeldungsmodalitäten stellt sich Ubuntu sofort zum Dienst. Wer nun bereits sein Laufwerk angeschlossen hat, wird es im Ubuntu-Dateimanager sehen. Diesen erreicht man oben über den Reiter „Orte“. Mittels angeschlossenen USB-Medien oder anderen Festplatten kann man nun Daten beliebig kopieren. Auch ein Brennen von CD-/DVDs ist mittels des integrierten Programms „CD-/DVD-Ersteller“ möglich. Dieses findet man wie alle anderen auch über das Menü am linken oberen Rand.

Hier noch einmal der Boot-Screen (Version 9.04). Die erste Option ist genau das Richtige: Ubuntu ausprobieren.

Hinweis: Wenn Sie sich später noch zur Installation entscheiden, können Sie das auch mitten aus dem laufenden System heraus machen.

Auch eine nachträgliche Neu-Formatierung ist dank GParted kein Problem.



5. Wichtige Protokolle

5 Auf Daten zugreifen … aber wie? Wichtige Protokolle im Überblick.

Viele Wege führen nach Rom. Aber nur wenige wirklich schnell. Welche Wege einfach und welche holprig aber dafür schnell sind um an Ihre Daten zu kommen soll jetzt geklärt werden. Der wichtigste Teil ist dabei natürlich der Zugriff im LAN. Wer hingegen von „extern“ zugreifen möchte, sollte direkt zum zweiten Teil dieses Kapitels springen.

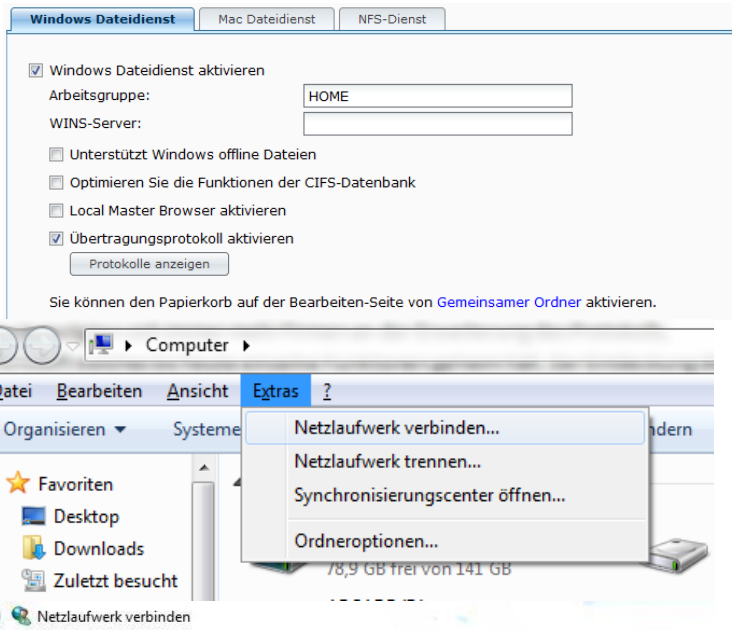
5.1 Zugriff über SMB/CIFS

Windows hat mehr zu bieten als nur die Anbindung als Netzlaufwerk. Doch zuerst die Basics. Die Theorie ist in Kapitel 1.7.4.

Gleich zu Beginn: Es ist nicht ohne weiteres möglich, die gesamte DS als ein Laufwerk mit dem PC zu verbinden. Einzig WebDAV bietet dies theoretisch an, jedoch mit anderen Einschränkungen und ausschließlich mit Zusatzprogrammen.

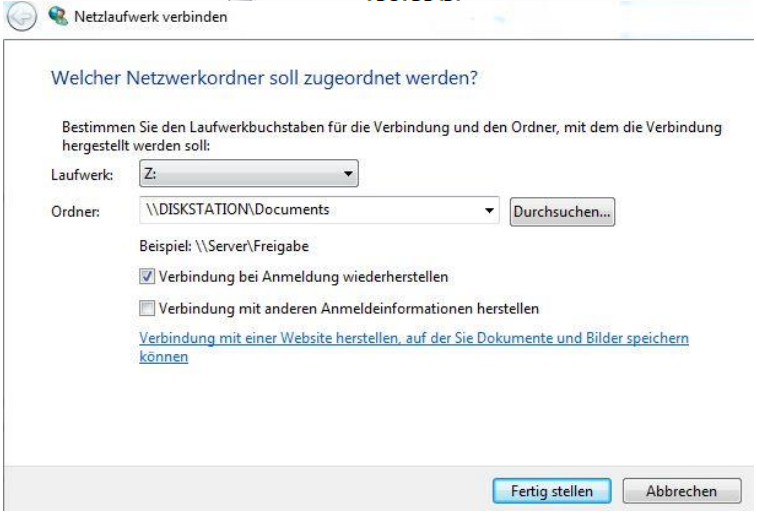
5.1.1 Mittels SMB Netzlaufwerke unter Windows verbinden

Also auf zu den Vorbereitungen. Auf der DS wird ein gültiger Benutzer mit Berechtigungen vorausgesetzt. Auch bezieht sich diese Beschreibung auf Windows XP und älter, insbesondere aber auf Windows 7. Falls sie eine andere Version einsetzen kann es punktuell zu Unterschieden im Einrichtungsprozess kommen.



Zunächst muss auf der DS sichergestellt werden, dass der Dienst aktiviert ist und die notwendigsten Einstellungen vorgenommen sind.

Unter „Win/Mac/NFS“ ist die Konfiguration des Sambas zu finden. Wichtig ist hier der Haken bei der Option „Windows Dateidienst aktivieren“ sowie eine Wert entweder bei Arbeitsgruppe oder WINS-Server. Die Arbeitsgruppe ist für Heimnutzer interessant und sollte mit dem übereinstimmen, was Windows unter „System“ (am einfachsten erreichbar über Windows-Taste + Pause-Taste) auflistet. In Unternehmen kommen hingegen häufig die als zweites aufgeführten Server zum Einsatz.



Nun zum PC. Hier beginnt alles im „Arbeitsplatz“ (XP) bzw. „Computer“ (Vista/7) (oder als Tastenkürzel Windows-Taste + E). In Vista/7 wird außerdem die Leiste mit den benötigten Schaltflächen versteckt; ein Druck auf „Alt“ ruft sie zurück.

Dort befindet sich unter „Extras“ die Option „Netzlaufwerk verbinden“.

Der Assistent von Windows 7 fordert nun den Pfad zur DS sowie den Namen des Ordners ein (\\DiskStation\Ordner). Die unteren Optionen bieten zum einen das automatische Wiederherstellen der Verbindung sowie die separate Eingabe den Zugangsdaten. Letztere sind allerdings bestimmten, teureren Windows 7 Versionen vorbehalten. Für alle anderen gilt: Benutzername und Passwort der DS identisch mit der des PCs halten. Das spart ggf. viel Nerven.

Und siehe da, ohne weitere Nachfragen verbindet Windows das Laufwerk insofern die Hinweise bezüglich der Zugangsdaten beachtet wurden.

Über einen Rechtsklick auf den Netzwerkpfad kann der Ordner für Offline-Verwendung auf die lokale Festplatte kopiert werden („Immer Offline verfügbar“). In diesem Fall werden die Daten wieder synchronisiert sobald eine Verbindung hergestellt werden konnte. Voraussetzung ist ein Haken in der Systemsteuerung des DSM („Unterstützt Windows offline Dateien“).

Zum Beenden der Partnerschaft dient der Button „Netzlaufwerk trennen“. Auch der Synology Assistant bietet eine Schritt-für-Schritt-Anleitung für dieses Vorgehen, mit dem Vorteil dass die Adresse dort vom Assistant bereits vorkonfiguriert wird.

5.1.2 Offlinedateien

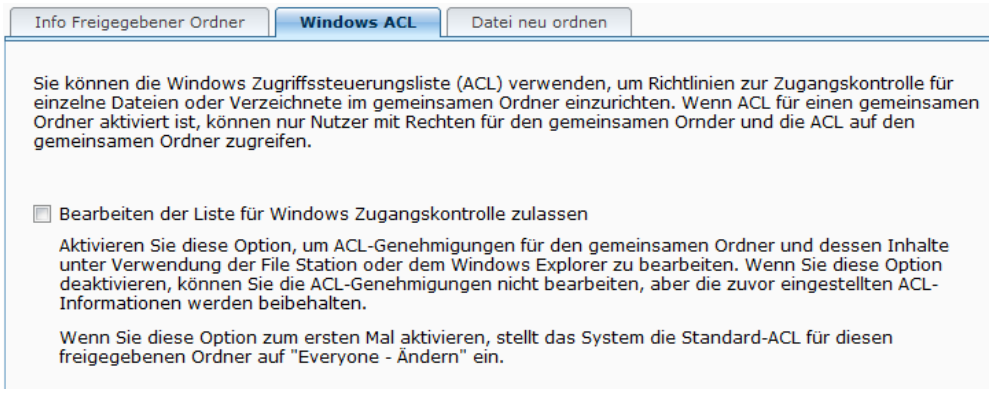
Unter Windows 7 können wichtige Netzwerkfreigaben auch Offline bereitgehalten werden. Das bedeutet natürlich, dass man wieder Festplattenspeicher verliert. Dafür wird selbstständig der Datenbestand auf Notebook/PC und Netzwerkfreigabe synchronisiert. Die nötigen Einstellungen sind im „Synchronisierungscenter“ unter „Offlinedateien verwalten“ zu finden. Windows 7 Starter, welches häufig auf Netbooks zu finden ist, ist davon leider ausgenommen. Auch im DSM muss die oben bereits erwähnte Option der Systemsteuerung aktiv sein.

5.1.3 Access Control Lists

Eigentlich ist diese mit „ACL“ abgekürzte Technologie nicht Windows-spezifisch. Doch eine DS kann sie bisher nur unter Windows nutzen. Der große Vorteil von ACL ist die präzisere Rechtevergabe. Linux kennt (wie Sie später noch genauer sehen werden) nur den Eigentümer einer Datei, dessen Gruppe und alle anderen. Mit ACLs sind aber die Berechtigungen für jeden Nutzer und jede Gruppe einzeln konfigurierbar.

Anmkerung: ACLs sind von ext4 abhängig, welches erst ab DSM 3.0 eingeführt wurde. Das Volumen muss daher mit dem DSM 3.0 oder höher erstellt worden sein.

Um ACLs zu aktivieren, erstellen Sie einen neuen „Gemeinsamen Ordner“ und gehen Sie in den zweiten Reiter „Liste für Windows Zugangskontrolle“ um die Berechtigung für den Nutzer „everybody“ zu aktivieren.

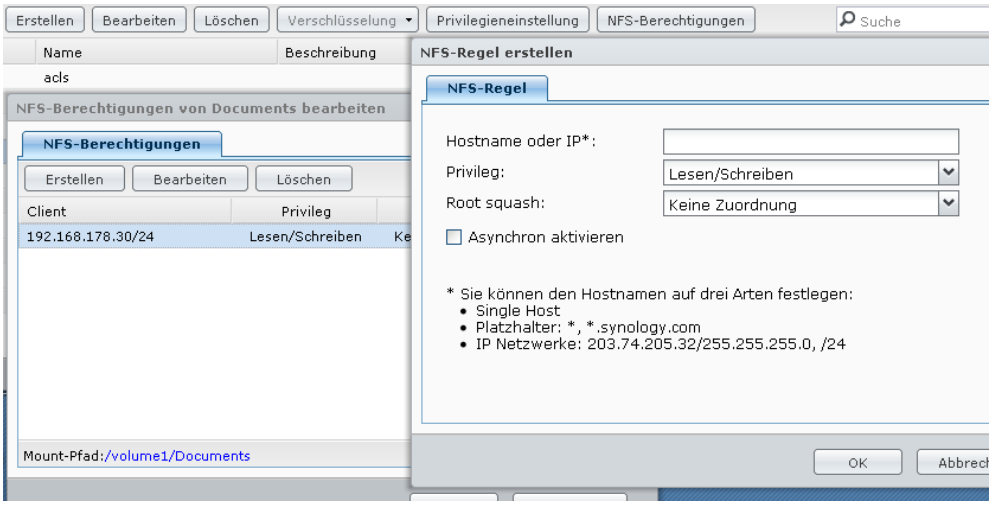


Die Berechtigungen lassen sich nun über einen Rechtsklick auf die Datei oder den Ordner im Windows Explorer konfigurieren. Ebenso greift die File Station auf diese Berechtigungen zurück.

5.2 NFS

Als nächstes folgt NFS. Aber Vorsicht: Auf Windows lässt sich NFS nur über Umwege betreiben. Eigentlich ist es in die DS implementiert um auch für Linux-Geräte entsprechende Kompatibilität sicherzustellen.

In der Regel bringt jede Distribution eigene Tools mit. Für die Kommandozeile gibt es ein Tutorial im englischen Wiki[52]. Nur auf eines möchte ich ganz besonders hinweisen: NFS hat eine etwas andere Struktur zur Authentifizierung, weshalb es eine komplett eigenständige Zugriffsregelung gibt. Diese lassen sich im DSM über „Gemeinsame Ordner“->„NFS-Berechtigungen“ auffinden und basieren auf den IP-Adressen der zugreifenden Geräte. **Ggf. vergebene Benutzer- oder ACL-Berechtigungen greifen hier nicht mehr!**



5.3 iSCSI

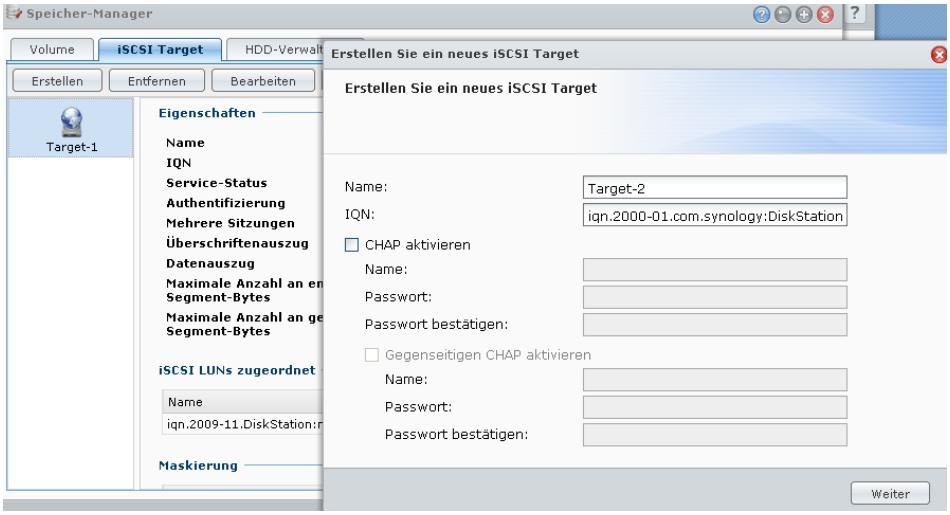
Jetzt wird es ein wenig technischer. iSCSI ist die Abwandlung des Hochgeschwindigkeitsprotokolls SCSI zur Verwendung über Netzwerke. Mehr zur Technologie gibt es unter 1.6.1.1. Ich beschränke mich daher auf eine Anleitung zum Verbinden.

[52] http://forum.synology.com/wiki/index.php/Mapping_a_Network_Drive#How_to_map_a_drive_using_a_Linux.2FUnix_Environment

5.3.1 iSCSI auf Windows einrichten

Die Einrichtung wird dank DSM und dem von Microsoft erstellten „iSCSI-Initiator“ sehr vereinfacht.

Im DSM bietet der Speicher-Manager einen Reiter „iSCSI LUN“ und ein „iSCSI Target“. Zuerst muss ein LUN erstellt werden, eine Art großer Speicherklotz, auf dem dann Targets liegen.

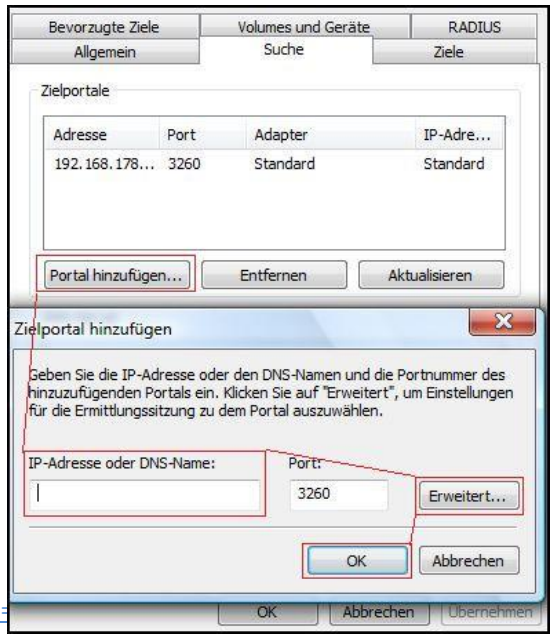


Hier ist der geöffnete DSM mit iSCSI-Target-Fenster zu sehen. Klickt man dort auf „Erstellen“, kann ein Name, sowie falls gewünscht die Authentifizierungsmethode angegeben werden. Auch gegenseitige Authentifizierung ist möglich. Dann muss sich nicht nur der Client beim Server, sondern auch der Server beim Client identifizieren. Auch kann hier eingestellt werden, ob mehrere gleichzeitige Verbindungen zugelassen werden sollen und noch vieles mehr.

Spannender, weil trickreicher ist aber die Einrichtung auf Windows-Seite. Vista und 7 besitzen dazu ein integriertes Dienstprogramm. Auf XP ist iSCSI auch möglich, benötigt aber eben jenen „iSCSI-Initiator“ als zusätzlich installierte Anwendung. Den Download findet man bei Microsoft.[53]

Ich möchte mich hier aber der Einfachheit halber nur auf Vista/7 beziehen.

Zunächst öffnet man dort den „iSCSI Initiator“, welcher in der Systemsteuerung zu finden ist.



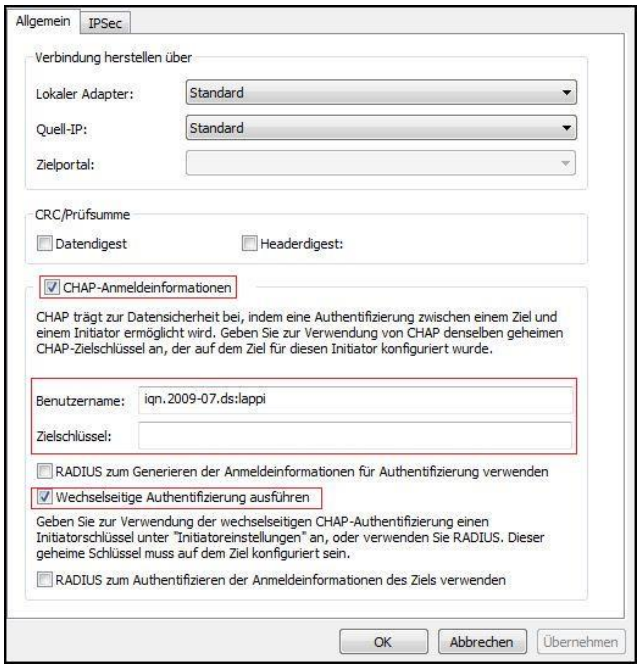
Es kann bei identischem Nutzername und Passwort auf Windows und DS/iSCSI-Volumen einfacher sein, die Schaltfläche „Schnell verbinden“ ganz oben auf dem iSCSI-Initiator, Reiter „Ziele“ zu nutzen. Dabei wird die Authentifizierung automatisch durchgeführt und mehrere Schritte außer das „Einrichten/Formatieren“ entfallen.

Ansonsten ist der Reiter „Suche“ hier die erste Anlaufstelle. Über „Portal hinzufügen …“ kann man die DS mit ihrer IP mit Windows bekannt machen. Der Port

[53] http://www.microsoft.com/downloads/details.aspx?familyid=befd1319f825&displaylang=en

ist übrigens bereits korrekt eingestellt, insofern man ihn im DSM nicht geändert hat. Auch eine Verbindung über das Internet mittels DDNS ist **theoretisch** möglich.[54] Bitte nutzen Sie den „Erweitert"-Knopf hier **nicht** um ihre CHAP-Daten einzugeben.

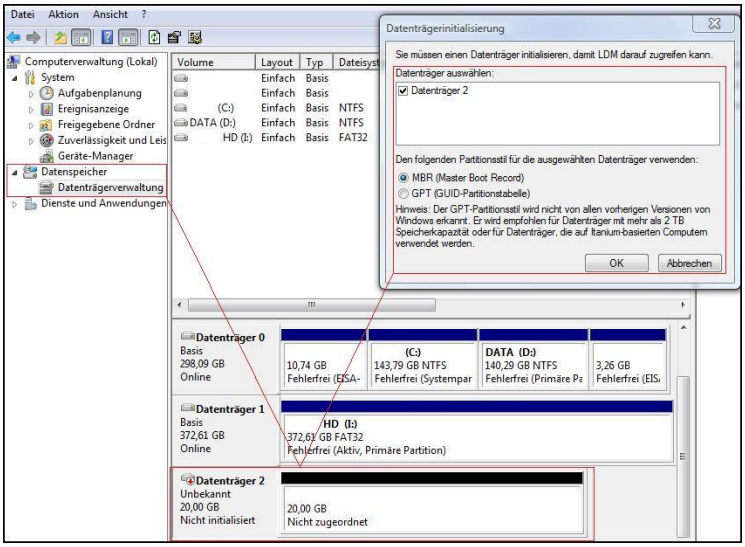
Nun geht es im Reiter „Ziele" weiter. Nach einem Klick auf „Verbinden" erscheint ein neues Fenster in welchem man auch einstellen kann, ob mehrere Verbindungen erlaubt werden sollen. Die Option darunter ist leider ein Trugschluss. Aus Erfahrung kann ich sagen, dass die Bezeichnung eigentlich falsch ist. Es sollte heißen "Verbindung beim Starten erzwingen", denn wenn die DS nicht erreichbar ist wird Windows nicht korrekt gestartet. Bei Laptops welche auch mal außerhalb des Netzwerks sind ist das natürlich denkbar ungünstig. Doch die Lösung liefert Microsoft gleich mit, ohne etwas darüber zu sagen: Windows (sollte) sobald ein iSCSI-Volumen erreichbar wird, dieses automatisch verbinden und dann den typischen "AutoStart" öffnen, ohne dass man jene fragwürdige Option einschalten muss.



Über den Knopf „Erweitert" links unten können die benötigten Daten für die CHAP-Authentifizierung eingegeben werden.

Als nächstes müssen Sie Windows noch erzählen, dass es ein neues iSCSI-Volumen gibt. Dies erfolgt am einfachsten über einen Rechtsklick auf „Computer" und dann „Verwalten". Es sollte nun die „Computerverwaltung" in Aktion treten. (Administratorrechte erforderlich)

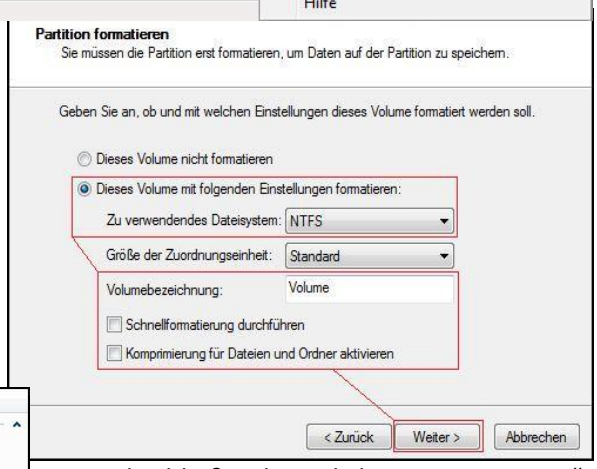
Hier sind nun unter „Datenspeicher -> Datenträgerverwaltung" alle bisherigen Festplatten und Partitionen zu sehen. Ganz unten findet sich dann ein Eintrag mit dem Status „Unbekannt" und „Nicht initialisiert". Beides wird sich gleich ändern. Über einen Klick darauf öffnet sich die „Datenträger-initialisierung". Erst ist eine Entscheidung zwischen „MBR" oder „GPT" nötig. Da es nicht



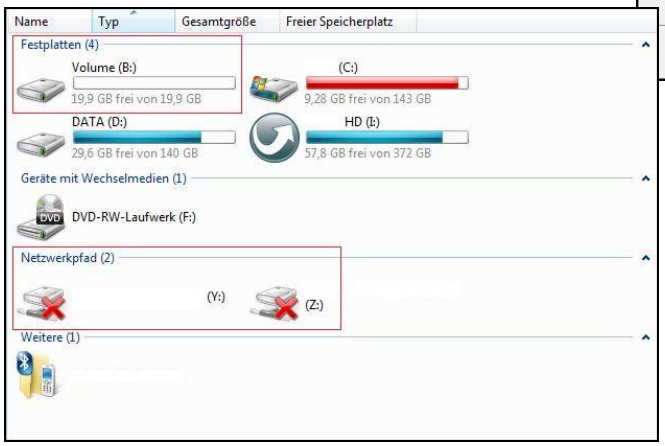
[54] Praktisch jedoch keinesfalls empfehlenswert. Es ist auch nicht dazu ausgelegt und bietet wenig Sicherheitsmechanismen zur verlustfreien, gesicherten Übertragung.

notwendig ist, GPT[55] zu verwenden, können sie die Voreinstellung „MBR (Master Boot Record)“ einfach belassen.

Mittlerweile ist der Datenträger zwar „Online“, jedoch „Nicht zugeordnet“. Also erstellen Sie mittels Rechtsklick einfach ein neues Volumen.



Jetzt möchte Windows den neuen Datenträger formatieren. Seien Sie unbesorgt, denn dies betrifft nur Ihr neues Volumen und nicht bereits genutzten Platz ihrer DS. Auch die standardmäßig verfügbaren Optionen „Schnellformatierung“ und „Komprimierung [..]“ sind zugänglich. Bei letzterem sollten Sie allerdings an die zu erwartenden Geschwindigkeitseinbußen denken.



Ein abschließender Blick in „Computer“ (ehemals „Arbeitsplatz“ in XP) sollte Ihre neue virtuelle Festplatte zeigen. Wie die Belegung meiner anderen Datenträger zeigt, war eine Erweiterung dringend Notwendig. Ich hatte mich, wie man sehen kann, für „B“ als Laufwerksbuchstaben entschieden. Hier wird auch gleich der wichtigste Unterschied zu einem Netzwerkpfad sichtbar: Die Einstufung als Festplatte erlaubt es Ihnen beispielsweise auch Programme dort zu installieren und alles andere zu machen, was ein Netzwerkpfad ihnen eigentlich nicht erlaubt.

Warum hat Synology diese Funktion eingebaut? Besonders im Business-Bereich ist es beliebt, selten genutzten Speicherplatz von echten Servern mittels iSCSI auf ein verhältnismäßig billiges NAS auszulagern und somit mehr Platz für wichtigeres zu lassen.

Auch haben Vergleichstests höhere Transferraten gezeigt. Während beim Lesen nur wenige Prozente Besserung zu erwarten sind, nähern sich die Schreib-Raten nahezu den Lese-Raten. Die Ursache hierfür liegt in der Geschichte von iSCSI: Das Lesen/Schreiben der Daten in Blöcken, wie bei Festplatten üblich, ist deutlich effektiver als das dateibasierte Abrufen welches beispielsweise SMB und AFP verwenden.

Auch unterstützt Synology für iSCSI spezielle Virtualisierungsfunktionen, was es unter einigen Plattformen besonders leistungsstark macht. Im Heimgebrauch trifft man dagegen eher selten auf iSCSI.

[55] Einziger Unterschied für den Nutzer ist die maximale Größe einer Festplatte. Bei MBR liegt diese Grenze bei 2 TB, einer heute durchaus realistischen Größe. Booten können allerdings nur PCs mit EFI-Bios von GPT-Festplatten.

Zusätzliche Lektüre finden Sie u.a. hier:

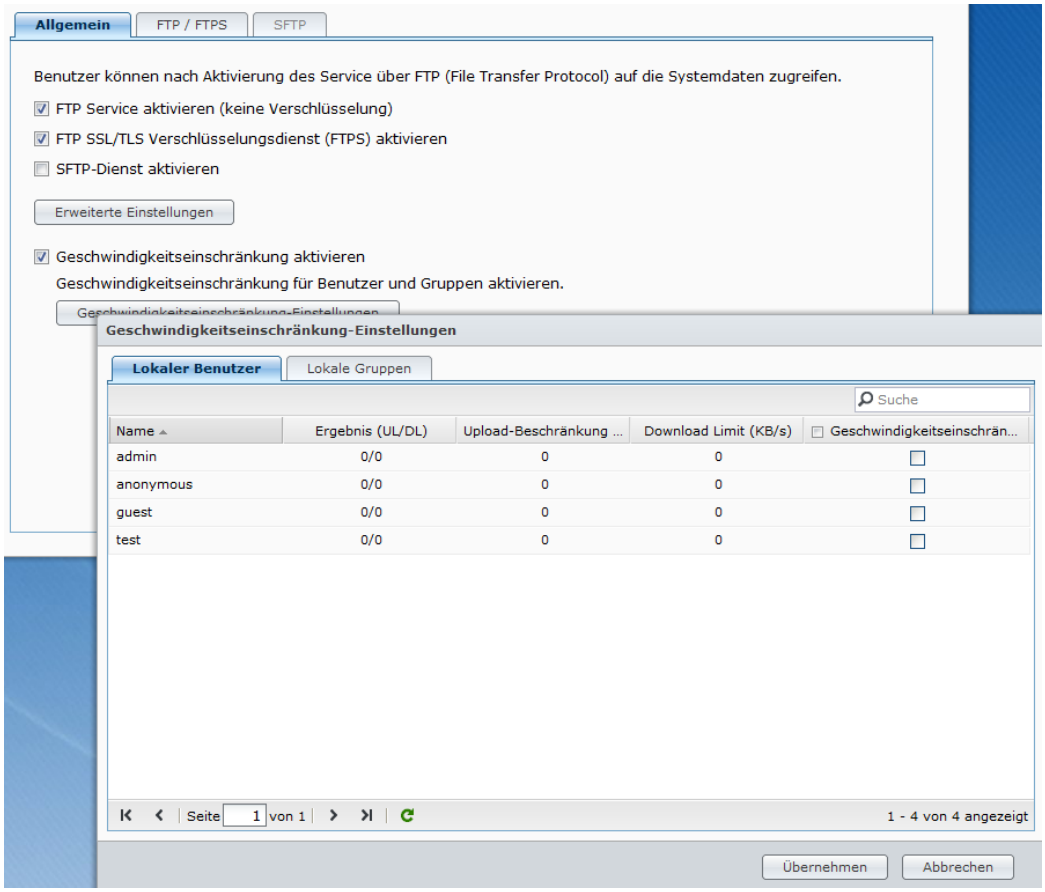
http://www.windowsnetworking.com/articles_tutorials/Connect-Windows-Server-2008-Windows-Vista-iSCSI-Server.html

5.4 AFP

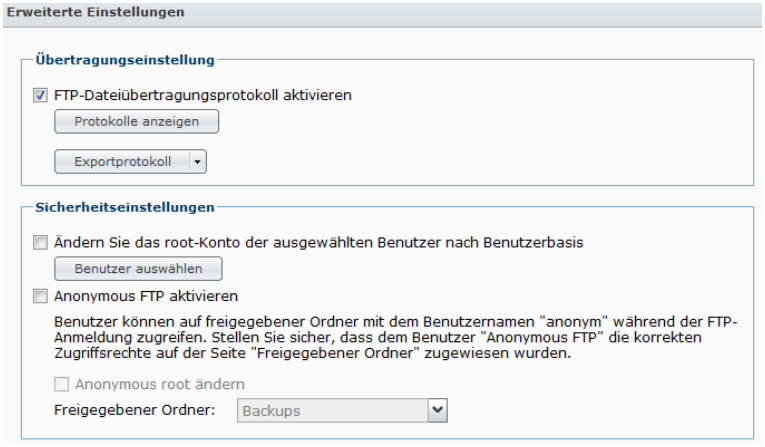
Für Mac-Nutzer ist außerdem das AFP-Protokoll zum Zugriff gegeben. Für Nutzer anderer Systeme wird sich AFP aber eher nicht lohnen, da es dort nur schwer zu konfigurieren ist, sofern man überhaupt die benötigten Systemkomponenten auftreiben kann. Im DSM muss dazu unter „Win/Mac/NFS“ die Option für AppleTalk aktiviert werden. Auch ist die Nutzung von „Time Machine“ als Backupprogramm möglich.

5.5 FTP

Weiter weg vom trauten Heim und dem dortigen NAS, stoßen viele Protokolle schnell an ihre Grenzen. Das Internet ist nicht nur ein deutlich größeres Netzwerk mit mehr Hürden, sondern stellt auch deutlich größere Anforderungen an Sicherheit der Daten sowie andere Aspekte der Datenübertragung über fremde Stellen. Zu Hause wissen Sie genau, über welchen Switch Ihre Informationen gehen, da es meist nur einen Weg gibt. Im Internet hingegen, steht man vor einer großen Reihe von Rätseln, die nur wenige Protokolle zu beantworten vermögen. Das wohl bekannteste ist FTP. Näheres zur Technologie gibt es in Kapitel 1.7.3. Interessanter ist an dieser Stelle, was die DS in Sachen Konfiguration hergibt.

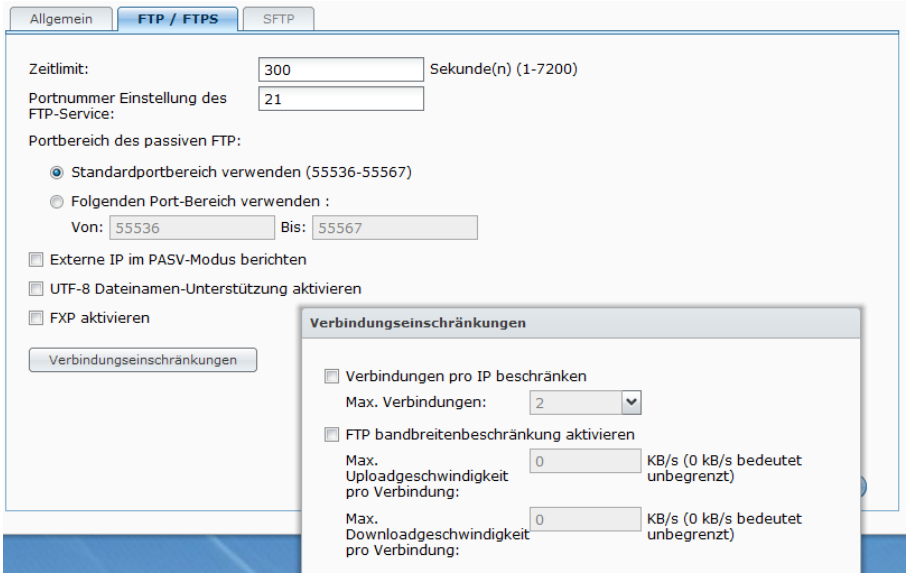


Speziell mit Firmware DSM 4.1 sind die Einstellungen in die Breite gegangen. Der Tab „Allgemein“ beinhaltet das Zuschalten der verschiedenen Zugriffsmethoden und Grundfunktionen. Dazu muss man nicht mehr viele Worte verlieren. Bei den „Erweiterten Einstellungen“ sind dann erste Optionen zu finden, welche nur in Problemfällen, bzw. mit entsprechendem Hintergrundwissen bedienbar sind.



Zunächst ist hier das Übertragungsprotokoll einschalt- und einsehbar. Hinter dem „root-Konto“ steckt das Einstiegsverzeichnis für den FTP-Client; mit „Benutzerbasis“ bezeichnet Synology den home-Ordner.

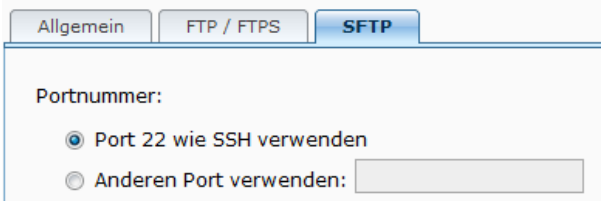
Anonymous FTP ist ein User für den keine Zugangsdaten benötigt werden. Dies kommt einem freien FTP-Downloadserver gleich, sollte daher nur verwendet werden wenn die Materialien wirklich für die Öffentlichkeit gedacht sind.



Während der FTP/FTPS-Dienst auf Samba basiert, ist das bei SFTP nicht der Fall. Aus diesem Grund sind die Einstellungen auch getrennt.

Konfigurierbar sind u.a. die Ports, sowie das Timeout für eine Verbindung. Die UTF-8-Dateinamen verbessern die Zeichendarstellung bei einigen Sprachen. Zusätzlich ist es bei FTP üblich, die Anzahl gleichzeitiger Verbindungen zu optimieren. Viele FTP-Clients bauen mehrere Verbindungen auf, um die Geschwindigkeit zu optimieren. Um dieses Verhalten nicht überhand nehmen zu lassen, kann die Bandbreite nicht nur per User (siehe vorherigen Abschnitt) sondern auch für den gesamten Dienst limitiert werden. Wird der Upload des eigenen Internet-Anschlusses zu stark beansprucht, kann das für Benutzer hinter diesem Anschluss unangenehme Folgen haben, bis hin zur gefühlten[56] Unerreichbarkeit von Webseiten.

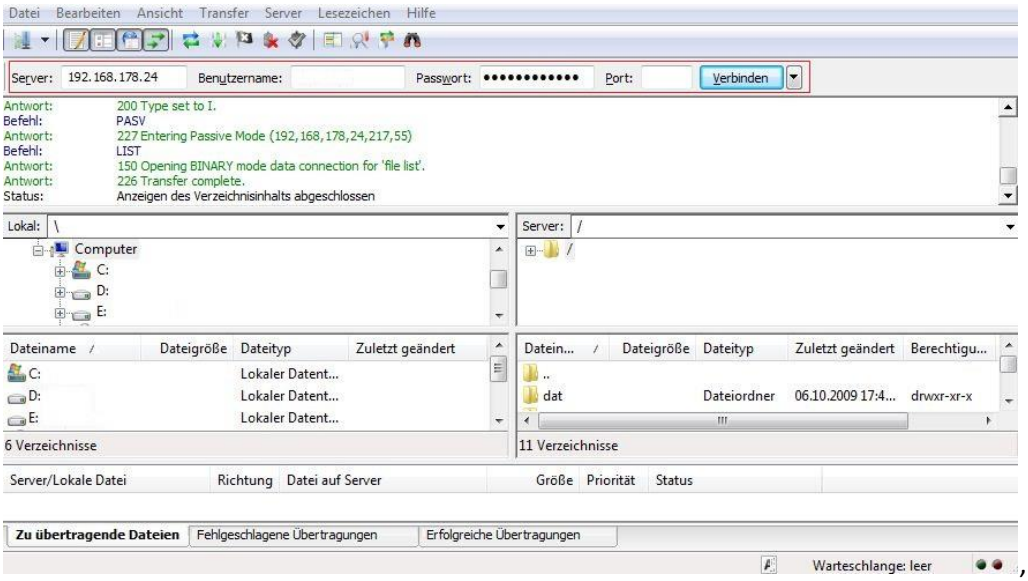
[56] Durch die Upload-Auslastung kann die Webseite zwar vom Server heruntergeladen, jedoch nicht wie vorher notwendig angefordert werden. Wer schon mal intensiv Torrents genutzt hat, kennt dieses Phänomen. Auch dort kann der Upload sehr effektiv ausgenutzt werden wenn man nicht aufpasst.



Schlussendlich steht noch der SFTP-Server im Raum. Er ist technisch etwas an den SSH-Server gebunden, weshalb es durchaus auch Wechselwirkungen zwischen beiden geben kann, insbesondere beim Modding. Neben Port 22 (SSH) kann jedoch auch ein anderer Port genutzt werden. In Anbetracht der häufigen Brute-Force-Attacken gegen SSH und auch FTP, ist dies bei FTP im allgemeinen wie auch bei SFTP im besonderen eine sehr gute Idee.

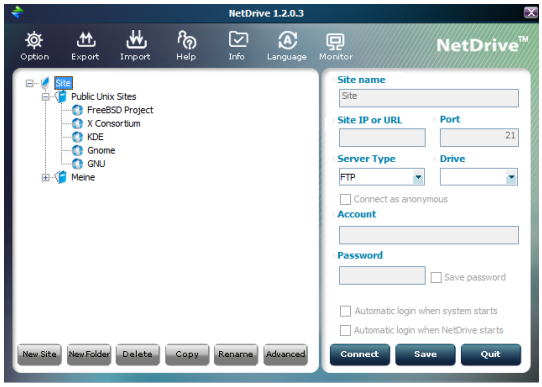
Übirgens lässt sich FTP (unverschlüsselt) auch als Netzlaufwerk in Windows einbinden. Ob das eine sonderlich gute Idee ist, muss jeder für sich entscheiden.

5.5.1 Zugriff mittels FileZilla



Die Benutzeroberfläche von FileZilla ist vergleichsweise übersichtlich aufgebaut, wenn man weiß welcher Kasten welche Funktion bedient. Allgemein zählt er zu den einfach bedienbaren Clients. Einige andere warten dafür mit technischen Raffinessen und Optimierungsmöglichkeiten auf (in dieser Kategorie wäre u.a. WinSCP zu nennen). Die oberste Leiste beinhaltet die nötigsten Eingabefelder für die Zugangsdaten. Im unteren Teil werden der Inhalt der eigenen Festplatte(n), sowie der Inhalt des FTP-Servers geöffnet. Dort kann mittels Drag & Drop mit Dateien gearbeitet werden. Bei der Fehlersuche ist unter anderem das Panel mit den FTP-Meldungen sehr hilfreich. Dort lässt sich meist die genaue Fehlerursache ablesen. Oder man beobachtet einfach einmal, was DS und PC so an Befehlen austauschen. Ganz unten ist die Warteschlagen beheimatet, welche die nächsten Dateien zur Übertragung anzeigt.

5.6 WebDAV



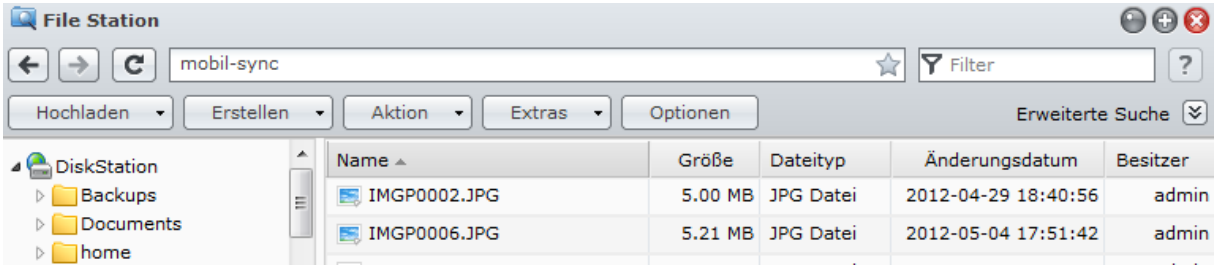
Eine lohnenswerte Alternative zu FTP ist WebDAV, eine Abwandlung von http um die Übertragung von Dateien zu verbessern. Es läuft daher auch auf dem Webserver und ist für den Einsatz über das Internet gedacht. Zu den besonderen „Schönheiten“ von WebDAV zählen Versionskontrolle, Port 80 zur Kommunikation (bei einer DS leider nicht nutzbar, da es nicht auf dem entsprechenden Webserver läuft, sondern auf dem System-Webserver welcher u.a. für die Anzeige des DSM zuständig ist) und eine breite Unterstützung von Betriebssystemen und Software. Windows 7 kann sich zwar prinzipiell mit WebDAV als Netzlaufwerk einbinden, stellt sich dabei aber etwas umständlich an und meckert gern über Zertifikate.[57] Doch für solche Fälle gibt es stets findige Entwickler: NetDrive[58] ist eine solche Software, welche eine komplette DS als Laufwerk einbindet. Man muss also nicht für jeden Ordner einzeln eine Freigabe erstellen. Leider ist diese nur für den Heimgebrauch kostenlos.

Die Einstellungen im DSM sind übrigens unter „Systemsteuerung“ > „WebDAV“ zu finden, da der Webserver für die Bereitstellung der Daten zuständig ist. Dort ist auch ein Zugriffsprotokoll aktivierbar sowie ein Zugriff für „Anonymous“ (ein Nutzer ohne Passwort). Auch ist WebDAV bei den Anwendungsberechtigungen vertreten. Man kann also steuern, ob ein Nutzer WebDAV überhaupt nutzen darf.

5.6.1 CalDAV

Zusätzlich unterstützt die WebDAV-Funktion auch die Erweiterung CalDAV. Es bietet damit die Möglichkeit, Kalender abzuspeichern. In Verbindung mit verschiedenen Geräten und Programmen können Kalender synchronisiert werden. Wer zusätzlich noch CardDAV (für Kontakte) haben möchte, muss derzeit zu anderer Software wie OwnCloud[59] greifen. Vorteil von OwnCloud ist außerdem ein Webbasierter Editor für Kalender und Kontakte.

5.7 File Station



Für einfachen und nicht exzessiven Dateizugriff kann auch die File Station das Mittel der Wahl sein. Eine Zeit lang existierte mit dem Datei Browser ein alternatives Tool im Rahmen des Desktop-Ansatzes, doch seit Version 4.0 ist die File Station auch auf dem DSM-Desktop ansässig und hat den

[57] Bei anderen Windows-Versionen weist Synology auf einen Patch hin, welcher angewendet werden sollte: http://www.microsoft.com/downloads/details.aspx?FamilyID=17c36612-632e-4c04-9382-987622ed1d64&displayLang=de

[58] http://www.netdrive.net/, kostenpflichtige Version für knapp 30 US$. Mögliche Alternativen: http://alternativeto.net/software/netdrive/

[59] Open Source mit kommerziellem Ableger, siehe: http://owncloud.org (Open Source) und http://owncloud.com (kommerziell)

kleinen Bruder verdrängt – und dabei auch einige Funktionen von ihm geerbt. Ein klares Zeichen der File Station ist aber das Java-Applet, welches den lokalen PC direkt in die File Station einbindet und sie so interaktiv macht. Alternativ kann man auch Dateien aus dem Windows Explorer (und ähnlichen Tools) direkt auf einen in der File Station geöffneten Ordner ziehen, was einen Upload der Datei zur Folge hat. Dazu kommen noch Funktionen wie Bild- und Dokumentenbearbeitung über Online-Dienste, ein eigener Bildbetrachter, das Erzeugen von Ein-Mal-Links ähnlich Dropbox und einige weitere Funktionen. Eines der besten Features zum Schluss: Auch Berechtigungen über Access Control Lists (ACL) können mit der File Station editiert werden.

5.8 Synchronisierung

In vielen Fällen hat man aber gar keinen Internetzugang und möchte trotzdem an Daten arbeiten die auf dem NAS gespeichert sind. Wenn das öfter der Fall ist, hilft nur eine Synchronisierung. Technisch gesehen hat man aber mehrere Möglichkeiten. Insbesondere bezüglich der „Software von Drittanbietern“ ist die folgende Übersicht stark reduziert und sicher nicht allgemeingültig. Ich hoffe, dass die Unterschiede gut erkennbar sind.

Software/Technologie	Vorteile	Nachteile
Synology Cloud Station	- In DSM integriert - Viele Plattformen unterstützt - Komprimierung und optionale Verschlüsselung	- Nicht für sehr große Datenmengen, da eher Bandbreiten-optimiert gearbeitet wird - Weiterer Dienst, weitere Portfreigabe - Beschränkung der Dateigröße
Windows „Offlinedateien“ (ab Windows 7 Professional; Windows 8 Pro)	- Leicht einzurichten, ins Betriebssystem integriert - Verwendet SMB/CIFS, kein zusätzlicher Dienst - In größeren IT-Umgebungen komfortabel administrierbar	- Nur auf Windows-Systemen - Synchronisierung meist nur im LAN
Software von Drittanbietern	- Zugriff erfolgt meist über vorhandene Dienste (FTP, SMB/CIFS, NFS, …)	- Synchronisierung meist nur im LAN - Selten Unterstützung für Mobilgeräte

5.9 Mobilgeräte

Für mobile Geräte mit den Betriebssystemen Android, Windows Phone und iOS gibt es von Synology verschiedene Anwendungen um den Zugriff zu vereinfachen: (nicht alle Anwendungen sind für alle Systeme verfügbar)

- DS file – Zugriff auf die Daten ähnlich der File Station. Außerdem werden auch erweiterte Funktionen wie betrachten und versenden unterstützt. Die Kommunikation erfolgt per WebDAV, entsprechende Portfreigaben sind somit erforderlich.
- DS photo+ – Dieses Gegenstück zur Photo Station ermöglicht das Abrufen und Hochladen von Fotos.

- DS audio – Wie in der Audio Station können hier Musiktitel gestreamt und eine angeschlossene Synology Remote (oder eine USB/Bluetooth-Soundkarte) gesteuert werden.
- DS cam – Die „VisualStation für Mobilgeräte“ könnte die Kurzbeschreibung lauten: Mobile, vereinfachte Ansicht der Kameras und deren Aufnahmen
- DS finder – Eine kleine nette Anwendung um den Status einer DiskStation zu überprüfen. Am hilfreichsten ist wohl die Funktion zum ferngesteuerten Hoch- (über WoL) und Herunterfahren.
- DS download – Anwendung um die Download Station unterwegs zu überwachen und mit Aufgabe zu füttern.
- DS cloud – Mobil-Komponente für die CloudStation zur Synchronisation.

Zusätzlich steht Geräten deren Browser sich als Mobil meldet eine spezielle Version des DSM sowie einiger Anwendungen zur Verfügung.

5.10 In ganz harten Fällen: VPN

Wer ganz sicher mit dem lokalen Netzwerk über das Internet kommunizieren möchte, greift am besten auf VPN zurück. Diese von Synology über das Paket „VPN Center“ angebotene Funktionalität bindet ein Gerät virtuell in das lokale Netzwerk ein und gewährt somit Zugang zu allen Protokollen wie im LAN – etwa SMB/CIFS oder auch AFP. Jedoch ist es nicht sehr einfach zu konfigurieren und man sollte durchaus ein wenig Zeit einplanen um sich in die Arbeitswelt eines VPN einzuarbeiten. Auch benötigt man für die Einrichtung meist Administratorrechte. Dafür kann man beinahe jedes Gerät und jedes Betriebssystem in ein VPN einbinden. Nur iSCSI ist allgemein nicht sehr verträglich für Fernverbindungen und damit auch für Verbindungen über ein VPN. Ist ein solches eingerichtet, verlaufen weitere Verbindungen recht unkompliziert bei unübertroffener Sicherheit.

Beachten sollte man jedoch, dass OpenVPN ein noch einmal deutlich sicherer ist als PPTP. Das von Microsoft entwickelte Protokoll hat einige bekannte Lücken welche auch aktiv ausgenutzt werden. Es gibt sogar einen Internetdienst welcher (für gutes Geld) PPTP-Verbindungen binnen 24h knackt.[60]

5.11 Fazit

Schlussendlich lässt sich wohl folgendes festhalten:

Zum Zugriff übers Web ist die File Station am komfortabelsten, zumindest zur Nutzung von wenigen Dateien. Bei größeren Mengen ist WebDAV deutlich unkomplizierter. Wer jedoch viel Wert auf Geschwindigkeit legt und dafür auch ein wenig Zeit in die Einrichtung investiert, greift stattdessen zu FTP. Außerdem ist man bei FTP nicht gezwungen, den System-Webserver freizugeben. Auf demselben Webserver läuft auch der DSM.

Über das LAN sollte man wahrscheinlich zur jeweils nativen Transportmethode greifen. Insbesondere Mac-Nutzer haben wenig Alternativen. Bei Linux hingegen ist es manchmal einfacher und komfortabler das zu nehmen was die Distribution so anbietet.[61] Und das muss, wie Ubuntu zeigt, nicht immer NFS sein.

[60] http://www.golem.de/news/vpn-security-passwoerter-knacken-fuer-200-us-dollar-1207-93555.html, Abgerufen am 31.7.2012, 21:57 Uhr

[61] Die grafische Oberfläche zur Einrichtung von SMB oder FTP-Verbindungen ist recht einfach zu bedienen, während NFS nur über die Kommandozeile zu konfigurieren ist.

iSCSI nimmt die Rolle eines Lückenfüllers ein und hat für die meisten Nutzer nur geringe Vorteile, die eine Verwendung angesichts der Nachteile nicht rechtfertigen. Es wird meist nur in Unternehmensanwendungen zwecks Virtualisierung verwendet. Viele andere Anwendungen sind damit hingegen nicht nutzbar.

Im Unternehmensbereich für den Fernzugriff ist VPN unverzichtbar und aus Sicherheitsgründen das Mittel der Wahl. Wer jedoch VPN geschäftlich nutzt, sollte überlegen die Einrichtung von Fachpersonal vornehmen zu lassen. Bei größeren Arbeitsgruppen sollte man auch den notwendigen Upload im Auge behalten. Da einem NAS die aufwändige Verschlüsselung einiges an Leistung abverlangt, kann auch ein VPN-Router eine gute Wahl sein.

Bild: Unter (cc)-Lizenz von „AMagill“ (Flickr)

5. Mitgelieferte Programme

6 Arbeiten mit den mitgelieferten Programmen

Einige Tools bekommt man beim Kauf eines Synology NAS mitgeliefert. Doch fühlen sich viele damit überfordert und brechen ihre Bemühungen schnell ab. Welche Möglichkeiten sich den Nutzern jedoch bieten, werde ich hier zeigen.

Die jeweils aktuellste Version findet sich auch auf der Webseite von Synology im „Download Center“[62]. Auch sollten möglichst Firmware und Programme ungefähr gleich „alt“ sein, da teilweise Funktionen genutzt werden welche Firmware-abhängig sind.

Es sind drei Anwendungen verfügbar:

- Synology Assistant zum Einrichten der DS inklusive Überspielen der Firmware
  - Erhältlich für Windows, Mac und Linux[63]
- Download Redirector für den Zugriff auf die Download Station
  - Erhältlich für Windows und Mac
- Data Replicator zum Anfertigen eines Backups der Daten vom PC auf eine DS
  - Erhältlich für Windows

Ich werde mich hier ausschließlich mit Windows befassen! Die Handhabung mit anderen Betriebssystemen unterscheidet sich aber meist nur geringfügig.

6.1 Synology Assistant

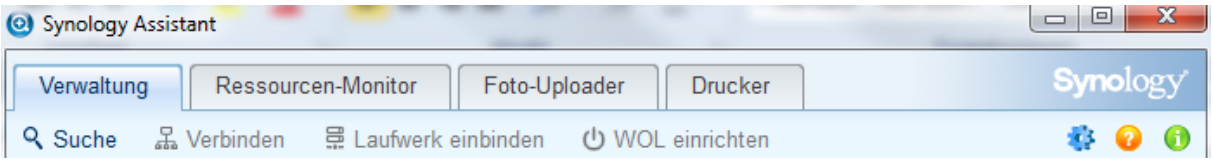
Um diese Software wird kein Nutzer herum kommen. Doch ich möchte gar nicht wieder zu weit vorgreifen. Lassen Sie uns einfach einen Blick darauf werfen.

Das heruntergeladene zip-Archiv enthält eine Installationsdatei welche den Assistant komfortabel auf dem System ausbreitet. Auch eine komplette deutsche Installation ist vorgesehen. Nach ein paar Klicks ist nun ein entsprechender Eintrag im Start-Menü zu finden.

Sobald man den Hinweis der Firewall abgearbeitet hat, sucht der Assistant im Netzwerk nach einer DS. Alle gefundenen Systeme werden nun in der Tabelle aufgelistet.

Hier ein Screenshot des oberen Teils der Oberfläche (GUI):

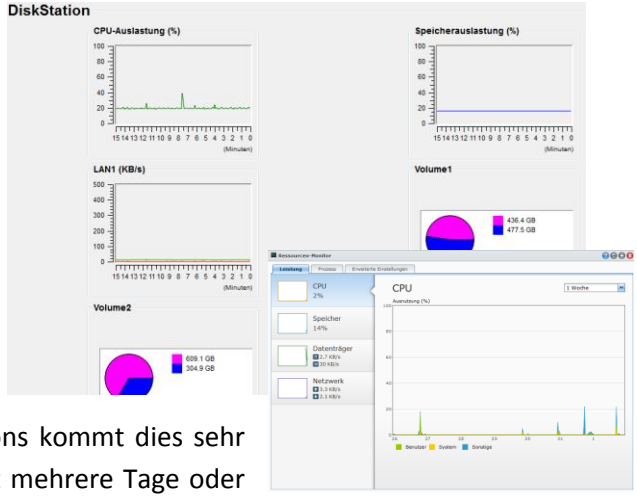
[62] http://www.synology.com/support/download.php?lang=de
[63] Offiziell unterstützt wird nur Ubuntu, doch auch auf anderen Distributionen läuft das Paket



Der Reiter „Verwaltung“ enthält die Tabelle mit allen DS im Netzwerk sowie die Optionen zum Verbinden mit dem DSM, dem Einbinden eines Netzlaufwerks, dem Hinzufügen eines Druckers welcher an der DS angeschlossen ist und dem Konfigurieren des Ressourcen-Monitors. Letzterer lässt sich anschließend über den dritten Punkt in der oberen Leiste ansehen. Unter „Installation“ lassen sich neue DS mit einer neuen Firmware bespielen.

Die Punkte der Installation sollten recht selbsterklärend sein, genauso wie die geführten Installationen der verschiedenen Funktionen unter „Verwaltung“.

Der in den Optionen angebotene Speichertest ist nur bedingt für den Normalgebrauch empfehlenswert, da nur umständlich die Testergebnisse erreichbar sind und der Vorgang die DS für eine längere Zeit (bei größeren DS mehrere Stunden) komplett lahm legt.



Zur Fernüberwachung dient der Ressourcen-Monitor. Mit dem gleichnamigen Programm des DSM (Bild rechts unten) kann dieser jedoch nicht mithalten. Er stellt die aktuelle Auslastung der wichtigsten Systempunkte dar, bietet aber z.b. keinen Zugriff auf die im DSM gespeicherten Leistungsverläufe.

Der Foto-Uploader kann das Skalieren der Bilder für Photo Station und Medienserver von der DS auf den PC verlagern. Gerade kleineren Disk Stations kommt dies sehr entgegen, bei großen Sammlungen kann dies sonst mehrere Tage oder gar Wochen in Anspruch nehmen. Bei leistungsstarken Geräten ist dies aber meist zu vernachlässigen, denn es erhöht sich auch die Übertragungszeit für die Bilder.

Unter „Drucker“ lassen sich der Printserver, sowie die Fax- und Scan-Funktion von Multifunktionsgeräten in Windows einbinden. Für letztere gibt es keine Alternative zur Konfiguration, denn die DiskStation arbeitet mit einem USB-Treiber dessen Gegenstelle nur im Assistant zu finden ist. Die Druckfunktion kann hingegen auch mit Windows direkt eingebunden werden.

6.2 Synology Download Redirector

Synology hat den Download Redirector vor einiger Zeit von der Webseite entfernt. Die Zukunft des Programms ist daher ungewiss, es gab jedoch auch noch keine endgültige Ankündigung. Die Verwendung der (durch private Entwickler erstellten) Browser-Plugins[64] ist ohnehin deutlich zeitgemäßer.

Der Download Redirector richtet sich an alle Nutzer der Download Station welche neue Vorgänge auch direkt über ihren PC ohne Umweg über den DSM eingeben möchten.

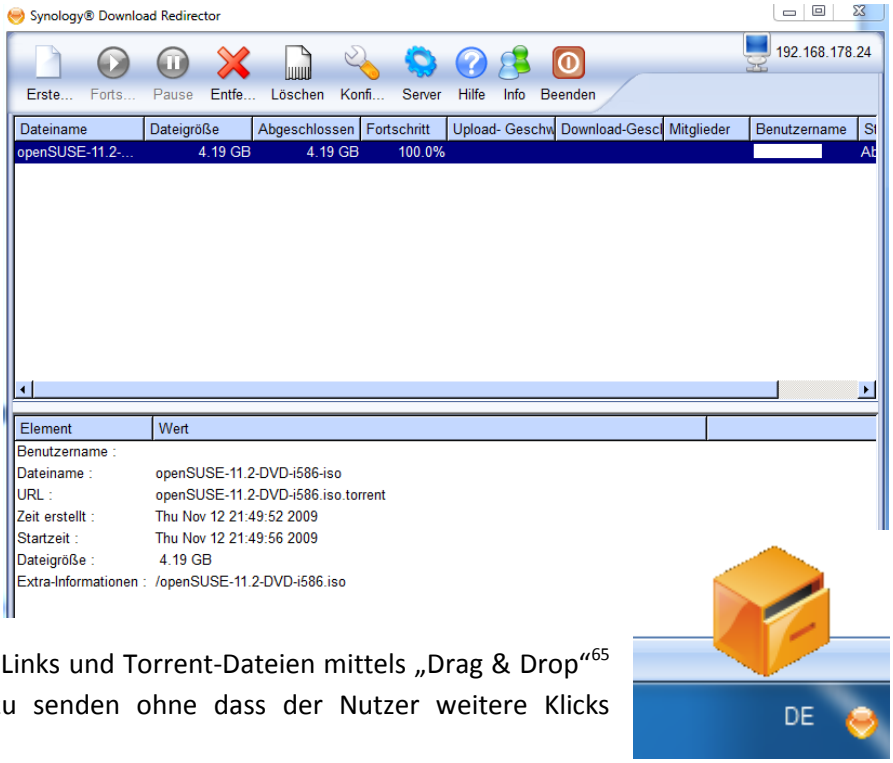
[64] Siehe Unterabschnitt im selben Kapitel

Beim ersten Start fragt das Programm sofort nach den Zugangsdaten für eine DS. Sind diese korrekt und die Download Station ist auf der Ziel-DS installiert, so wird sofort die Liste älterer Vorgänge geladen und neue können hinzugefügt werden.

Die Oberfläche ist wieder recht simpel gestaltet. Allerdings sind allerdings die Beschriftungen einiger Icons beim Übersetzen zu lang gewesen und wurden „gekürzt“.

Unter „Konfiguration“ können neue Zugangsdaten angegeben werden und unter „Server“ lassen sich die wichtigsten Einstellungen der Download Station einsehen.

Der „Erstellen“-Dialog bietet Optionen für einen neuen Download-Auftrag. Viele Optionen basieren auf einer älteren Firmware, weshalb die Download Station mehr Funktionen besitzt.



Wenn das Programm nicht benötigt wird minimiert es sich zum einen in den sogenannten „System-Tray“, also den Bereich neben der Uhr, und behält außerdem eine orangene Kiste im Vordergrund welche von Synology „Drop Zone“ genannt wird. Wer sich an dieser stört kann sie mittels Rechtsklick auf besagtes Icon im Tray deaktivieren. Andernfalls bietet sie die Möglichkeit, Links und Torrent-Dateien mittels „Drag & Drop“[65] auf die DS als Auftrag zu senden ohne dass der Nutzer weitere Klicks vornehmen muss.

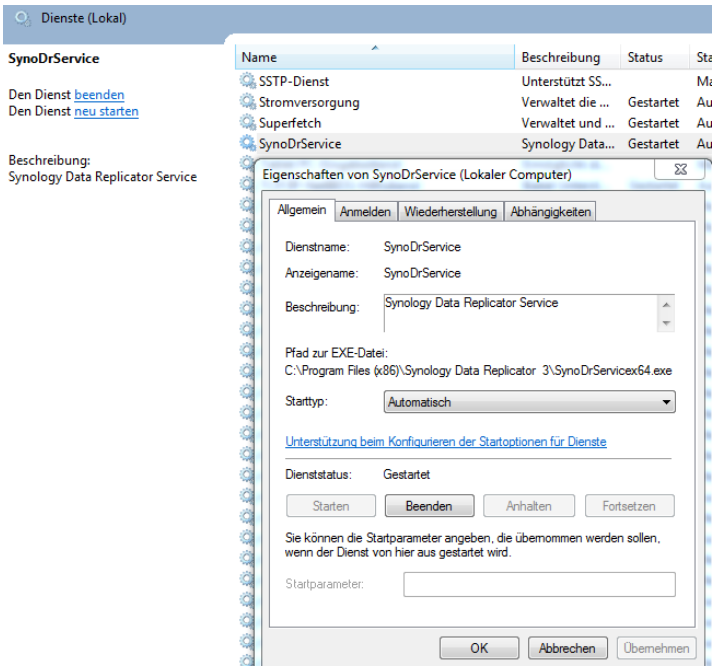
6.2.1 Alternative: Browser-Plugins

Für Chrome und Firefox gibt es, wie im Eingangstext bereits angesprochen, Plugins um Downloads mit noch weniger Aufwand hinzuzufügen. Diese Plugins werden nicht durch Synology offiziell entwickelt, sondern sind in den Händen von freiwilligen Entwicklern. Das Plugin für Chrome[66] wird am stärksten weiterentwickelt und unterstützt auch https.

Für Firefox gibt es zwei Anläufe, der Entwicklungsstand dort ist recht unterschiedlich und Anpassungen an neue Firefox-Versionen gibt es eher sporadisch. Welche besser ist muss jeder für sich entscheiden, der Funktionsumfang ist weitestgehend identisch.[67]

[65] Aus dem Englischen: Ziehen und fallen lassen, also ein beliebiges Element auf dem Bildschirm mit der linken Maustaste aufnehmen und diese Taste solange gedrückt halten bis der gewünschte Zielort erreicht ist.
[66] Chrome Webstore: https://chrome.google.com/webstore/detail/onhbegdkgonhlokobjefolhpoidcnida
[67] SynoLoader für Firefox: https://addons.mozilla.org/de/firefox/addon/synoloader/
SynoExt für Firefox: https://addons.mozilla.org/de/firefox/addon/synoext/

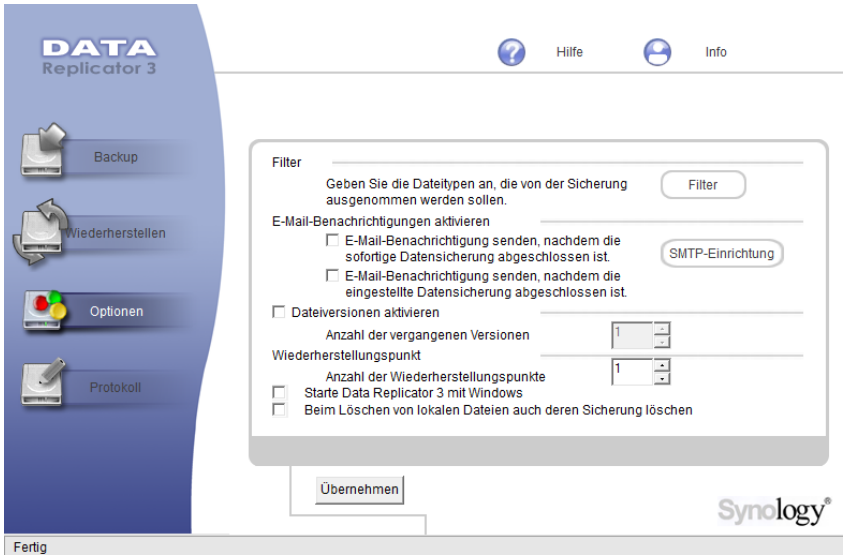
6.3 Data Replicator



Fehlt noch eine Anwendung zum Anlegen von Backups. Einige Hersteller legen Lizenzen von spezialisierten Herstellern bei, Synology setzt wiederum auf eine Eigenentwicklung.

Die komplexeren Möglichkeiten beginnen hier schon bei der Installation. So befinden sich in dem Ordner „application“ alle benötigten Dateien um den Replicator auch ohne Installation zu verwenden.[68] Die „normale“ Installation ist im Ordner „install“ als „Setup.exe“ zu finden.

Die beiden Kommandozeilenfester welche während der Installation kurz zu sehen sind stammen von einem Systemdienst welcher vom Data Replicator verwendet wird um auch im Hintergrund auf Abruf agieren zu können. Wer sich in den tieferen Bereichen von Windows auskennt und einmal die „services.msc“ ausführt wird ihn bald als „SynoDrService“ enttarnen können. Ich möchte jedoch darauf hinweisen, möglichst nicht an diesen Einstellungen zu drehen.



Beim ersten Start präsentiert die Anwendung ihre „Optionen“-Seite. Viele der hier zu treffenden Entscheidungen sind wichtig für den sicheren Gebrauch und sollten nicht überlesen werden.

Ein Backup ist schnell eingerichtet. Bei der Eingabe des Zielpfades ist es empfehlenswert den etwas längeren Weg über die Option „Synology Server“ zu gehen, da hier mehr Optionen bereit stehen und sogar eine Einschätzung der Sicherheit ihrer Daten aufgrund der Zugangsberechtigungen gegeben ist.

Nach der Wahl der zu sichernden Dateien muss noch die Methode angegeben werden. „Sync“ überprüft ständig auf Änderungen an den entsprechenden Dateien und kopiert wenn notwendig. Hier ist zu beachten, dass bei gleichzeitigem Bearbeiten einer Datei durch mehrere Benutzer Konflikte entstehen können, welche durchaus auch einen Datenverlust verursachen. Eine echte Synchronisation über mehrere Geräte hinweg sollte man eher der Cloud Station überlassen.

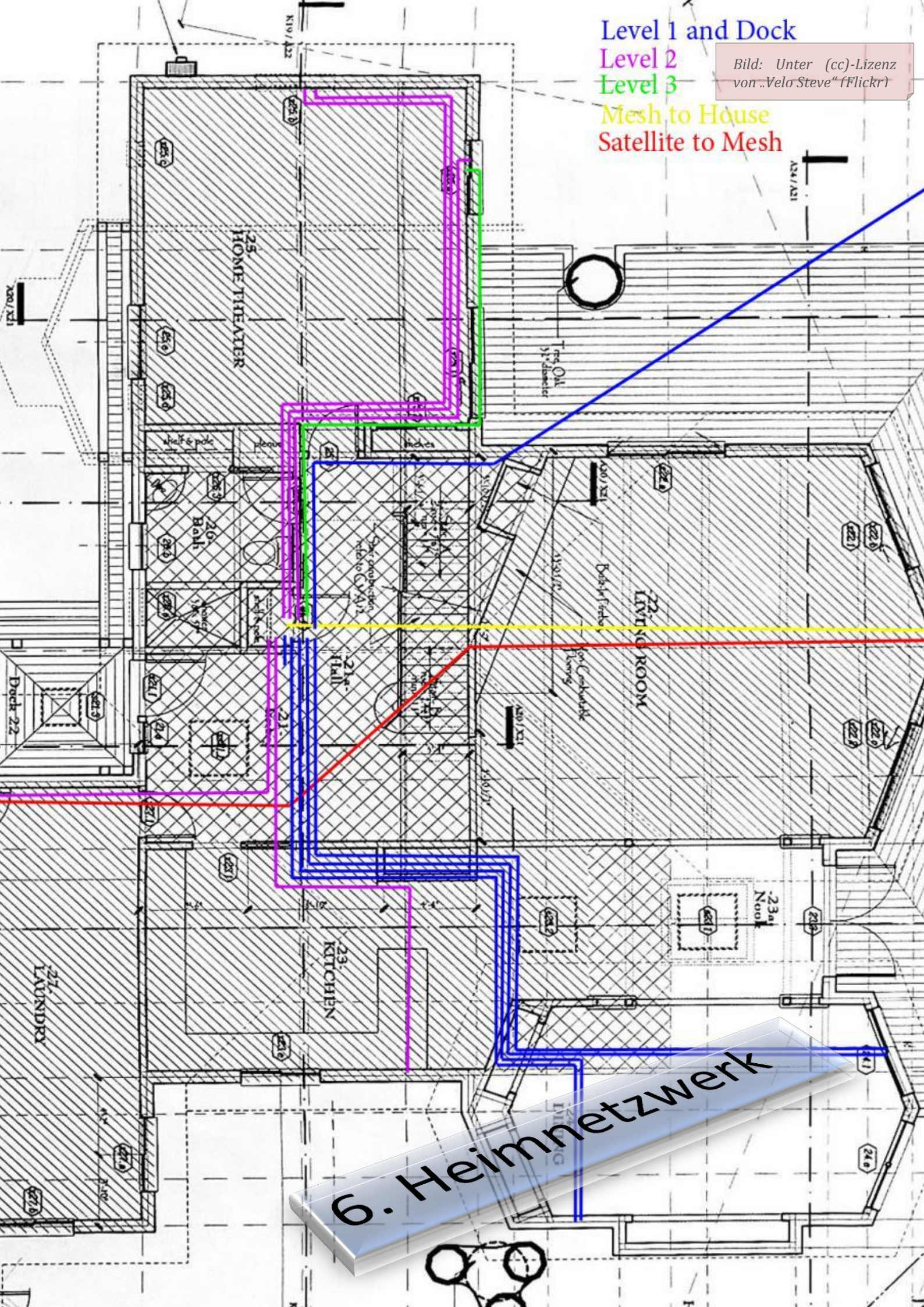
[68] Im Produktiveinsatz sollte man das aber nicht tun!

Andernfalls kann der Replicator auch zeitgesteuert in Aktion treten und dann aktiv werden wenn Sie vielleicht gerade beim Mittagessen sitzen und kurz Ihren PC anlassen. Beides ist kein Problem, da wie bereits besprochen ein Systemprozess verwendet wird, der auch tiefere Einblicke zulässt und sich schlafen legt wenn er nicht akut benötigt wird.

Das integrierte Protokoll schreibt alle Vorgänge mit, sodass sämtliche Änderungen und Backups sowie Fehler nachvollziehbar sind.

6.4 Cloud Station & Photo Station Uploader

Als Abschluss dieses Kapitels könnte man auch noch die Software der „Cloud Station“ erwarten. Da diese jedoch sehr eng an die entsprechende Software für die Disk Stations gebunden ist, befindet sich auch der Client in Kapitel 2.8.1. Selbiges gilt für den „Photo Station Uploader“, der in Kapitel 2.6.2 zu finden ist.


Level 1 and Dock
Level 2
Level 3
Mesh to House
Satellite to Mesh
Bild: Unter (cc)-Lizenz von „Velo Steve“ (Flickr)
25. HOME THEATER
26. Bath
22. LIVING ROOM
21. Hall
23. KITCHEN
23a Nook
27. LAUNDRY
Deck 22
6. Heimnetzwerk

7 Die DS im Heimnetzwerk – Netzwerke aufbauen und erweitern

Die meisten Nutzer kaufen sich eine DS entweder wenn sie ein neues Netzwerk beispielsweise für ein neues Haus aufbauen oder wenn sie ihr bisheriges erweitern möchten. In beiden Fällen gilt es aber eine Vielzahl von Dingen im „Drumherum“ zu beachten.

7.1 Techniken und Standards

Wie beim gesamten Aufbau dieses Handbuchs möchte ich auch in diesem Kapitel zunächst etwas genauer auf die wichtigen Technologien und Standards eingehen.

7.1.1 Cat und Kabel

Wenn es um Geschwindigkeit geht, gibt es im Heimbereich keine wirkliche Alternative zu Twisted Pair Kupferkabeln. Glasfaser sei an dieser Stelle explizit als nicht für den Heimgebrauch üblich genannt. Twisted Pair steht für verdrillte Adernpaare. Damit wird ein „Übersprechen“ von Signalen weitestgehend verhindert. Bei den mittlerweile üblichen hohen Frequenzen und Datenraten können Signale von einer Ader auf eine andere per Magnetfeld einwirken. Legt man die Adern parallel und ungeschützt direkt nebeneinander erhält man schon nach einigen Zentimetern keine brauchbare Übertragung mehr.

In Weitverkehrsnetzen, insbesondere bei der kostengünstigen Anbindung von Endkunden, steht für viele Internetprovider auch das Koaxialkabel als Kupferkabel zur Verfügung, aber das nur am Rande.

Die Abschirmung ist der wohl wichtigste Faktor bei Kupferkabeln. Physikalisch gesehen gerät man bei Kupfer mittlerweile an gewisse Grenzen. Bei Glasfaser hat die Entwicklung in den letzten Jahren hingegen erst so richtig Fahrt aufgenommen. Um diese Grenzen bei Kupfer so weit wie möglich auszureizen, werden einzelne Adern bestmöglich voneinander getrennt.

Bei Twisted Pair wird zwischen einer inneren und äußeren Schirmung unterschieden. In den USA werden nach wie vor viele Kabel ohne innere Schirmung verlegt, in Europa ist das nicht der Fall. Das ist auch wirtschaftlich sinnvoll, weil die Kosten für die Kabel meist keinen großen Anteil an den Gesamtkosten haben wenn man die Verlegung professionell erledigen lässt. Unter innerer Schirmung versteht man eine Folie/ein Drahtgeflecht um die verdrillten Adernpaare. Je besser diese Paare voneinander getrennt sind, desto höhere Frequenzen können auf den Kabeln genutzt werden. Und höhere Frequenzen bedeuten nun einmal mehr Geschwindigkeit. Um für die verschiedenen Geschwindigkeiten und Standards vergleichbare Grundlagen zu schaffen, gibt es Kategorien, Englisch „categories“, kurz daher „Cat“.

Die älteren und deutlich schwächeren „Cat“-Versionen 1-4 werden heute nicht mehr für Heimnetzwerke verwendet und sind nur bei alten Überlandleitungen zu finden. Sie sind nur schlecht oder gar nicht geschirmt und bieten keine (aus heutiger Sicht) brauchbaren Übertragungsraten.[69]

Die neueren Normen 5, 5e, 6 und 7 sind für höhere Frequenzen ausgelegt und machen eine gute Abschirmung Pflicht. Ab relativ kurzen Distanzen von 10 Metern sind bei Cat 5 allerdings bereits Einbußen zu verzeichnen. Daher sollte auch mit Blick auf die Entwicklung höherer Übertragungsraten Cat 6 bei neuem Ankauf bevorzugt werden, um Zukunftssicher zu arbeiten. Der Standard für Cat 7 ist noch nicht alt, hat mit Blick auf 10GBit Ethernet aber neue Steckverbindungen bekommen. Entsprechende Komponenten sind noch rar und teuer, lohnen sich daher aktuell im Heimgebrauch

[69] Beispiel: Cat 1 ist vergleichbar mit Klingeldraht …

nicht. Das Einziehen neuer Kabel ist häufig ein Kraftakt; der Aufpreis für bessere Kabel ist dagegen ziemlich gering. Seit einigen Jahren werden darüber hinaus alte Cat 5e-Kabel auch als Cat 5 bezeichnet. Daher Vorsicht: Nicht überall wo Cat 5 draufsteht, ist auch Cat 5 drin.

Welcher Norm Kabel entsprechen ist meist darauf als Aufdruck vermerkt. Wenn die üblichen Mindestangaben zu CAT und Abschirmung fehlen, sollte man etwas genauer hinsehen.

Wer professionell Kabel, insbesondere für Büroräume, verlegen lässt, sollte abschließend auf eine Prüfung der Verbindungen bestehen.

7.1.2 Fast und Giga

Gemeint sind hiermit verschiedene Ethernet-Standards. Gemeinhin in Heimnetzwerken verwendet sind Fast- und Gigabit-Ethernet. Sie sind Synonyme für die Geschwindigkeiten 100 und 1000 Megabit/s (Mb/s, im Gegensatz zu MB/s). Außerdem gibt es noch das veraltete 10 Mb/s und das deutlich teurere 10 Gigabit/s. Letzteres kommt bisher nur in Unternehmen zum Einsatz. Große NAS (Synology: XS/XS+ Reihe) können beispielsweise mit mehreren dieser Schnittstellen ausgerüstet werden – den passenden Geldbeutel vorausgesetzt.

Der größte Unterschied bei 100MBit/s und 1GBit/s ist die Verwendung aller 8 Leitungen eines Netzwerkkabels bei Gigabit, während Fast Ethernet nur auf 4 dieser Leitungen angewiesen ist und die anderen als „Reserve“ nicht belegt. Wenn Gigabit also mal nicht zustande kommt, kann das an Kabelproblemen liegen. Sind nicht zu viele Adern betroffen, wird dann nämlich auf Fast Ethernet zurückgegriffen.

7.2 Der Anfangspunkt: Der Router

Am Anfang steht meist der Router, denn er ist entweder bereits vorhanden, wird vom Provider gemietet, oder als „kleines Werbegeschenk“ mit verabreicht. Wenn sie dennoch einen neuen Router kaufen, sollten Sie auf die folgenden Punkte achten.

Anzahl der Ports: Wenn Sie nur wenige Geräte besitzen, werden Sie die meisten direkt an den Router anschließen. Überlegen sie sich daher genau, ob sie nicht doch zu einem Modell mit 4 statt nur 2 Anschlüssen greifen sollten. Auch die Geschwindigkeit auf diesen Ports (Gigabit, Fast Ethernet) ist zu berücksichtigen. Bei mehr Geräten lohnt es sich auch aus Sicht des Stromverbrauchs einen großen Switch zu verwenden statt mehrerer kleiner Geräte. Aber auch das ist wieder von den örtlichen Gegebenheiten abhängig. Leider noch nicht flächendeckend im Handel sind Gigabit-Schnittstellen.

NAT/Firewall: Alle Router blockieren, von Haus aus, ungefragt eingehenden Datenverkehr ohne weitere Beachtung rigoros. Doch gerade wer einen Server für welchen Zweck auch immer in seinem

Netzwerk betreibt, wird hier vor Probleme gestellt, denn dieses Verhalten führt zu einer Nicht-Erreichbarkeit des Dienstes. Wer dann nicht auf die Einstellungen der Firewall Einfluss nehmen kann, steht schnell vor einem Problem. Doch dies ist in der Regel nur bei billigen Geräten der Fall. Aufschluss darüber erlaubt meist der Blick in das Handbuch des Geräts, welches schon vor Kauf auf der Internetseite des Herstellers abrufbar sein sollte. Wird eine entsprechende Funktion erwähnt, braucht man sich keine Sorgen zu machen (Stichworte: NAT, Port Forwarding, Firewall).

Wireless LAN: Besonders teuer im Nachrüsten ist Wireless LAN, kurz WLAN. Da meist ein sogenannter Access Point benötigt wird wenn der Router diesen Dienst nicht bietet, können die Anschaffungskosten schnell in die Höhe gehen. Diese Geräte sind durchaus mal teurer als ein Router. Nach ca. 5 Jahren sollte man unter Umständen dann prüfen, ob neue Endgeräte nicht auch einen neuen Router mit besserem WLAN rechtfertigen. Die Hersteller und Entwickler legen alle paar Jahre einen Standard nach mit dem die Geschwindigkeit und häufig auch die Reichweite erhöht wird.

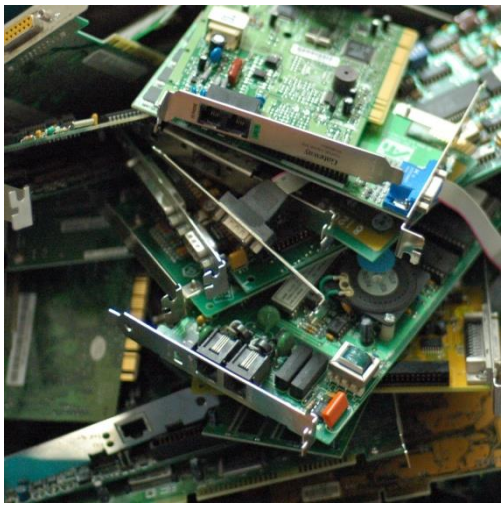
Jeder Router hat dann noch eine Reihe von Zusatzfunktionen, die nützlich sein können. Insbesondere im Telefonie-Bereich ist viel Spielraum vorhanden. Auch mit Kindersicherungen wird gern geworben. Doch aus Sicht eines NAS-Besitzers und engagierten Netzwerkers sind die oben aufgeführten am wichtigsten.

7.3 Die Hauptstation: der PC

Die zentrale Steuerfunktion übernimmt nach wie vor der PC. Oder wie viele davon auch angeschlossen sein werden …

Da auch Standard-PCs sehr komplexe Geräte sind, ist auch ihre maximale Übertragungsrate im Netzwerk von vielen Faktoren abhängig. Zum einen ist da natürlich die Festplatte, denn fast alle Daten werden dort abgelegt oder gelesen. Bei alten Platten kann bereits weit unterhalb der Gigabitrate Ende der Fahnenstange sein. Doch halbwegs aktuelle Festplatten schaffen weit über 120 MByte/s[70], während bei Gigabit in der Regel, je nach Protokoll, „nur“ bis zu 105 MByte/s machbar sind. Des Weiteren muss der Transport natürlich auch koordiniert werden. Ist der Prozessor daher zu schwach, kann trotz neuer Festplatte schnell der Spaß vergehen.

Bild: Unter (cc)-Lizenz von Jeff Kubina (Flickr)



Ein ganz heikles Thema sind auch die entsprechenden Netzwerkkarten. Wenn der PC nur interne PCI-Schnittstellen besitzt, kommt eine weitere Engstelle ins Spiel. Doch glücklicherweise ist PCI seit einiger Zeit vom erweiterten PCIe abgelöst. Hier liegt die maximale Übertragungsrate deutlich höher. Genauer gesagt arbeiten hier 16 Spuren die jeweils bis zu 2 GBit/s transportieren können. Wer nun vor der Auswahl einer neuen Karte steht und seinen Prozessor entlasten will, sollte zu einer etwas teureren Markenkarte suchen und nicht die erstbeste nehmen. Während die Chips von bekannten Herstellern wie Intel viel Rechenarbeit selbst machen, koordinieren andere Billig-Chips nur die Rechenarbeiten.

[70] Eine Ausnahme bilden dabei die besonders stromsparenden („grünen“) Serien. Dort sind ca. 100MB/s üblich.

Nun sollten Sie sehr genau wissen, was Ihr PC leisten kann und wo Sie eventuell noch investieren müssen.

7.4 Die Verteiler: Switch und Hub

Nun da Sie ungefähr wissen, wie viele Geräte angebunden werden wollen, können Sie mit der Planung der Verteiler, also der Switche beginnen. Da Sie als Heimnutzer keine besonderen Ansprüche haben sollten, sind eigentlich nur die Anzahl der Ports und die erreichbare Geschwindigkeit wichtig. Zu den Ports genügt der simple Ratschlag: kalkulieren Sie den Wachstum Ihrer IT-Landschaft ein. In den letzten Jahren sind z.B. Fernseher zu den vernetzbaren Geräten gekommen. Bei der Geschwindigkeit heißt das Stichwort Gigabit. Der wie schon weiter oben angesprochene, geringe Preisunterschied rechtfertigt nicht die Wahl eines langsameren Gerätes.

Fast gänzlich aus dem Handel verschwunden sind Hubs. Ein Hub vervielfältigt ein Paket wenn es ihn erreicht und leitet es an alle angeschlossenen Partner weiter. Ein Switch kennt nach kurzer Zeit die Endgeräte an jedem Port und leitet die Pakete nur dorthin weiter, wo es auch wirklich von Interesse ist. Dazu kommen dann noch die teuren „Managed“-Geräte. Dort können diverse Parameter konfiguriert werden, die in Unternehmen Übersicht und Performance sicherstellen. Preise von 100€ aufwärts machen diese Geräte aber für Heimnutzer ohne IT-Wissen uninteressant.

7.5 Die Kabel

Das Thema Kabel versteckt sich eigentlich schon in den „Techniken und Standards“ aus Kapitel 7.1. Ich möchte aber noch auf den Unterschied zwischen „Patchkabel“ und „Verlegekabel“ hinweisen. Letztere sind ein ganzes Stück teurer, sind aber für das Verlegen in Wände und Decken vorgesehen. Durch die stärkere Abschirmung können da auch mal Stromkabel gekreuzt werden. Die Kabel sind dafür insgesamt dicker, benötigen also mehr Platz. Doch bei den Wandsteckdosen für Ethernet hat man mit Patchkabeln keine leichte Aufgabe – die meisten sind auf die dickeren Adern von Verlegekabeln ausgelegt. Angesichts der Einsatzdauer dieser Kabel ist es keine gute Idee, da an wenigen Euros zu sparen wenn hinterher, bei verputzter Wand und verlegtem Kabel, die Leitung auf einigen Adern tot ist oder Störeinflüsse große Paketverluste verursachen.

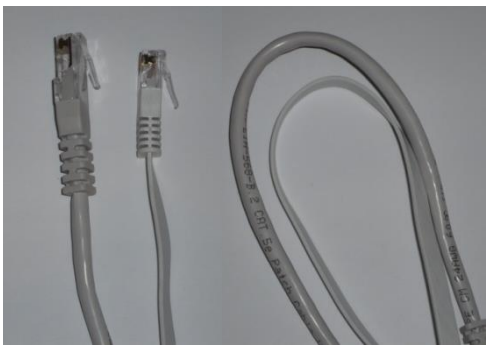
Doch eigentlich wichtig ist der nächste Abschnitt, denn Kabel zu verlegen ist nicht sonderlich schwer. Aber was, wenn keine Kabel so verlegt werden können?

7.6 Alternativen zum klassischen Kabel

Insbesondere in älteren Gebäuden kann man nicht einfach zum Bohrer greifen um neue Kabel durch alte Mauern zu ziehen. Daher werden in letzter Zeit immer mehr Alternativen zu klassischen Kabeln gesucht und auch gefunden.

7.6.1 Flache Kabel

Noch gar nicht so lange sind besonders flache Kabel auf dem Markt. Dabei werden die Adern möglichst eng aneinander gelegt um die maximal benötigte Höhe des Kabels zu verringern. Leider wird dabei die Abschirmung gegen äußere Einflüsse so weit wie nur irgend möglich verringert und auch die Verdrillungen eingeschränkt.



Doch die Vorteile sind schwer zu übersehen. Selbst dort wo nie Kabel vorgesehen waren, lassen sich solch flache

Kabel gut unter Teppichen verstecken und unter Fenstern hindurch führen.

Wäre da nur nicht das liebe Geld. Selbst vergleichsweise dicke Kabel kosten noch rund vier Mal so viel wie hochqualitative Standardkabel gleicher Länge. Auch ist die Länge hier viel kritischer als bei Standardkabeln.

7.6.2 Lichtwellenleiter (LWL)

Schaut man weiter in Richtung High-Performance trifft man unter anderem auf Lichtleiter. Als flächendeckender Ersatz für Kupferkabel im Heimbereich bieten sie sich aufgrund der Preise und der eingeschränkten Verlegemöglichkeiten derzeit noch nicht an. So lassen sich LWL nicht einfach kürzen und haben vorgeschriebene Biegeradien. Stattdessen werden immer mehr Kunststoffleiter verkauft. Technisch gesehen sind Glasfaser das Maß der Dinge mit dem größten Spielraum für zukünftige Entwicklungen. Es gibt auch „Medienwandler“, welche Kupferkabel mit Glasfaser verbinden. Alternativlos sind Glasfasern auch in Umgebungen mit vielen Elektromagnetischen Störeinflüssen, etwa in Fabriken. Alle anderen hier aufgeführten Alternativen lassen sich dort ebenso wenig wie klassische Kupferkabel einsetzen. Möchte man auf größeren Grundstücken die 100m überschreiten, die den Maximalausbau von Ethernet ohne aktive Komponente darstellen, kommt man ebenfalls schwer an Lichtwellenleitern vorbei.

7.6.3 WLAN

Warum überhaupt noch auf Kabel vertrauen? Viele Laptops bringen eigene Onboard-Chips mit und für den Rest gibt es kleine USB-Karten von der Größe einer Geldmünze. Doch auch hier ist nicht alles Gold was glänzt. Um mal schnell im Wohnzimmer ein paar Fotos zu zeigen mag WLAN noch ausreichen, doch zum Anfertigen eines Backups sollte man dann doch den Gang zum Kabel nicht scheuen. Auch werden Hausbesitzer schnell die Nachteile von Stahlbeton zu spüren bekommen. Der Funkkontakt über mehrere Etagen ist nur schwer zu erreichen oder gar unmöglich. Als billige Kurzzeitlösung ist WLAN also durchaus geeignet. Aber bei größeren Datenmengen oder Entfernungen kommt man um eine kabelgebundene Lösung nicht herum.

7.6.4 Powerline

Was sich anhört wie eine futuristische Alternative zum Stromkabel überträgt in Wahrheit Daten über selbige. Während Computernetzwerke in vielen Häusern immer noch den Kürzeren ziehen und nur sekundär bedacht werden, ist eine vernünftige Stromanbindung unabdingbar. Die Idee ist ebenso einfach wie genial: Warum nicht die bereits bestehende Struktur nutzen? Die Probleme die dabei auftreten liegen allerdings ebenso einfach auf der Hand. Nur minimale Einwirkungen auf die Stromversorgung sind zulässig um nicht gleich den PC in eine „Wäschemaschinen-Abschuss-Vorrichtung“ zu verwandeln wenn man mal auf das Netzwerk zugreifen will.

Besonders schön illustriert wurde dies in einem Forenbeitrag von jahlives[71]:

„Es ist beim Stromnetz einfach so, dass es bei der Qualität sehr stark auf Installation der Adapter ankommt. Wenn an der gleichen Steckdose neben dem Adapter noch Mehrfachsteckleisten oder sonstige Netzteile hängen, dann kannst du die Geschwindigkeit rauchen. Gleiches gilt wenn z.B. im gleichen Stromnetz ein Gerät wie ein Haarföhn benutzt wird. Dann bricht die Übertragungsrate stark ein und es kommt zu ziemlich massiven Paketverlusten (also nicht föhnen und gleichzeitig eine DVD streamen wollen 🙂 *“*

[71] http://www.synology-forum.de/showthread.html?p=25319#post25319

Auch hier ist die Entwicklung recht rasant, weshalb ich keine Zahlen nennen möchte. Jedoch sollte man die Nachteile nicht unterschätzen und nur in aussichtslosen Fällen auf Powerline zurückgreifen. Preismäßig gehört Powerline zu den günstigeren Alternativen (insbesondere weil man kein zusätzliches Kabel benötigt), wenn auch bei weitem nicht so billig wie Standardkabel.

Auch als DSL-Alternative war Powerline kurzzeitig im Einsatz. Der Pilotbetrieb wurde aber schnell wieder eingestellt als man bemerkte, wie sich die Überlandleitungen plötzlich in riesige Antennen verwandelt hatten. Auch im heimischen Einsatz lassen sich Störungen bei Amateurfunk und Radio durchaus messen; allerdings nur innerhalb der gesetzlichen Normen. Wer einen Amateurfunker in der direkten Nachbarschaft hat oder ohnehin einen schlechten Radioempfang hat, tut sich und seinen Nachbarn trotzdem keinen Gefallen mit Powerline.

7.7 Das vernetzte Haus

Der Blue-Ray-Player lädt Trailer aus dem Internet nach und in der Küche dudelt ein Internetradio. Wann gehen wohl die ersten Waschmaschinen online? Spaß beiseite. Aber die zunehmende Vernetzung ist doch überall spürbar. Mehr Geräte mit mehr Funktionen und höheren Anforderungen werden zwangsweise in das eigene Netzwerk eindringen. Bei der Wahl dieser kann nur eine Fachzeitschrift behilflich sein, denn das Testen einer großen Vielfalt von Geräten ist zeitraubend und nicht zuletzt natürlich auch eine Kostenfrage. Doch auch bei solchen Tests sollte man nicht schnell auf den „Testsieger“ steigen, sondern lieber ein wenig im Internet forsten und Meinungen in Foren einholen ob die gewünschte Kombination auch zusammen das macht was sie soll. Auch die Aufschrift „DLNA zertifiziert“ heißt noch nicht das auch alles so läuft wie man es sich vorstellt.

Doch um auch in der Zukunft mithalten zu können lässt sich nicht viel tun, da man nie weiß was als nächstes kommen wird. Leerrohre in den Wänden für neue Kabel sind ein guter Anfang. Auch eine Planung im Voraus ist meist hilfreich um genauestens zu bestimmen was benötigt wird. Schlussendlich bleibt mir nur ein Rat: Kaufen Sie IT-Geräte und Zubehör wenn Sie es brauchen und ärgern Sie sich nicht wenn zwei Monate später schon der Nachfolger angekündigt wird.

Bild: Unter (cc)-Lizenz von „mroach“ (Flickr)

8 Das Linux auf der DiskStation

8.1 Die Geschichte von Linux

Meine kleine Exkursion beginnt 1983. Wer bereits ein wenig über die Ursprünge von Linux weiß, mag sich wundern, warum ich so früh beginne, denn zu diesem Zeitpunkt gab es noch nicht mal die Idee hinter Linux. Doch lange vor Linux entstand das GNU-Projekt. Richard Stallman arbeitete zu dieser Zeit am MIT und wenn man damals Software bestellte, bekam man sie meist in Form des Quelltextes, damit man notfalls das Programm an den eigenen Computer anpassen konnte. Doch nun wurde es mehr und mehr Mode, die Software in binärer Form, also als direkte Dateien, auszuliefern um die eigenen Codes nicht zugänglich zu machen. Die Idee hinter GNU war die Schaffung eines freien, UNIX-ähnlichen Betriebssystems, welches mit allen nötigen Tools kommen sollte, um das System vom Kern an, für die eigenen Bedürfnisse und technischen Grundlagen anzupassen. Es dauerte mehr als ein Jahrzehnt, bis diese Grundbausteine fertig waren. GNU konnte viele frühe Erfolge einfahren, doch es hatte ein großes Problem: Es besaß keinen eigenen Kern, einen sogenannten Kernel. Stattdessen waren Nutzer immer noch darauf angewiesen, das „Halb-Betriebssystem“ auf einem bestehenden (kommerziellen) System wie den damaligen UNIX-Varianten zu installieren. Auch wenn sich viele nicht daran störten, wurden die Debatten um alternative Kernel immer intensiver, bevor Linux entstand. Auch wenn Linux nie ein richtiger Teil des GNU-Projekts wurde (Richard Stallman und sein Team arbeiteten stattdessen weiter am GNU HURD, dem ersten eigenen Kernel), basiert es trotzdem sichtbar auf GNU und setzt auch viele der dafür entwickelten Komponenten ein. Daher nennt man es auch „GNU/LINUX“.

Der Linux Kernel entstand fast ein Jahrzehnt nach den ersten Meilensteinen des GNU-Projekts. Der finnische Student Linus Torvalds (Universität Helsinki) wollte ursprünglich seinen PC besser verstehen und baute sich ein Terminalprogramm mit dem er Zugriff auf die Universitätsrechner bekam. Doch irgendwann bemerkte er, wie hardwarenah er programmierte und dass daraus ein kleiner Kernel gewachsen war. Im Sommer 1991 schrieb er dann in einer Usenet-Newsgruppe einen kleinen, mittlerweile legendären Bericht über seine Arbeit und forderte die Leser auf, ihre Wünsche an ihn zu richten. So wuchs schnell die Zahl der Interessierten und Aktiven, da sich viele über diese Neuentwicklung freuten, welche nicht dieselben Kinderkrankheiten aufwies, wie die bisher entwickelten Lösungen. Schließlich wechselten sogar Entwickler der alternativen „Minix“ und „HURD“ -Systeme zum Linux-Projekt über, was dessen Gründer, Andrew Tanenbaum ziemlich aus der Fassung brachte.

Als Linux weiter wuchs, vergrößerte sich auch das Interesse an einer Lösung, Linux für Nicht-Entwickler zugängig zu machen, denn bisher musste Linux nach wie vor an das eigene System angepasst werden. Auch entwickelten sich Terminals, wie die Shell, welche auch nach wie vor beim Modding[72] einer DiskStation zum Einsatz kommt, zu grafischen Oberflächen weiter. So entstanden die ersten Distributionen. Diese besitzen z.B. eigene Installations-Routinen um den Nutzer durch diesen komplizierten Prozess zu begleiten. Des Weiteren bekommt man mit Distributionen fertige Anwendungen mitgeliefert, sodass man sofort loslegen kann.

[72] umgangssprachlich für modifizieren, also das Anpassen des Systems über die vom Hersteller gegebenen Möglichkeiten hinaus, teilweise auch mit Verlust der Garantie behaftet

8.2 Warum Linux?

8.2.1 Linux unter GPL-Lizenz

Richard Stallman gründete im Zuge von GNU die „Free Software Foundation“. Eine nicht-kommerzielle Organisation, welche sich neben der Verwaltung der GNU-Entwicklung auch mit der Schaffung der GPL-Lizenz beschäftigte. GPL steht für „General Public License“. Ein großer Teil des Linux-Kernel steht unter dieser Lizenz. Software, welche unter GPL steht, kann von Interessierten ohne Probleme geändert und angepasst werden, da der gesamte Quellcode zur Verfügung steht. Also könnte man zum Beispiel in GPL-Software einen Bug beheben und die neue Eigenentwicklung veröffentlichen. Doch die GPL besagt weiter, dass dieses neue Programm erneut frei zu Verfügung stehen muss.

8.2.2 Linux ist frei verfügbar

Diese GPL-Lizenz macht es schließlich möglich, dass jedes Individuum und jede Firma ein eigenes Linux auf dem freien Kernel aufsetzen kann. So entstanden bereits Linux-basierte-Systeme für verschiedenste Geräte, wie Handys, Fernsehrekorder und Großrechner. Daher nutzt auch Synology für die DiskStations ein Linux. Doch aufgrund der GPL ist der Code, auf welchem dieses Betriebssystem basiert, frei verfügbar. Für mehr Informationen lohnt sich ein Blick in den Supportbereich von Synology oder auf die entsprechende Sourceforge-Projektseite[73].

8.2.3 Linux ist modular

Während Betriebssysteme wie Windows oder Mac als Ganzes programmiert werden und später auch so laufen, besteht Linux aus vielen kleinen Einzelteilen, welche zusammen arbeiten um ein großes Ganzes zu ergeben. Bei Linux werden kleinste Funktionen in verschiedenste Mini-Programme aufgebrochen. Auch die Lautstärke besteht so aus verschiedenen Teilen. Was sich wie die unnötige Verschwendung von System-Ressourcen anhört, bietet bei genauem ansehen einen großen Vorteil: Bleibt einer dieser Bestandteile stecken oder erliegt einem Ausnahmefehler, kann er dies melden, ohne dass gleich das gesamte System betroffen ist und möglicherweise zusammenbricht. Außerdem macht es dies für Entwickler sehr viel einfacher, da der Quellcode viel übersichtlicher und einfacher zu warten ist.

8.2.4 Linux ist sicher

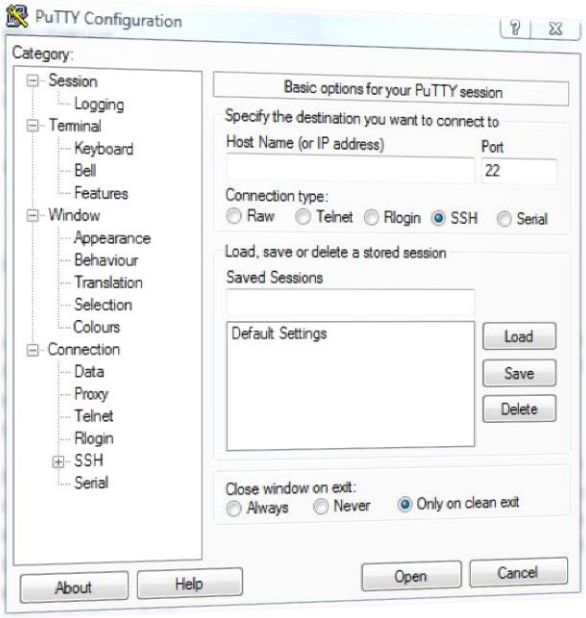
Viele der bereits genannten Punkte spiegeln sich auch hier wieder. Denn wie soll man einen Virus programmieren, wenn man nie weiß, was das Zielsystem genau am Ende bereithält. Ein Virus, welcher für x86-Architektur gebaut wurde (x86 ist ein normaler Heimcomputer), hat unter x64, also bei 64-Bit-Systemen schlechte Karten. Wer sich hingegen als Angriffsstelle die Distribution aussucht, wird zwangsweise später genauso auf einer anderen Distribution landen, welche anders aufgebaut ist. Auch die rege Community trägt ihren Teil dazu bei. Denn werden Probleme entdeckt, dauert es meist nicht lange, bis es entsprechende Lösungen gibt. Solche Sicherheitsrelevanten Themen werden meist in abgeschlossenen Chats diskutiert (schließlich sollte nicht jeder wissen, wo Probleme liegen). Wer nach noch einem weiteren Punkt schaut, stößt wieder auf den Modularen Aufbau. Denn wenn ein Virus ein Modul attackiert, ist die Wahrscheinlichkeit hoch, dass man am Ende nur einen winzigen Teil zerlegen konnte und das eigentliche System nach wie vor seinen Dienst verrichtet. Nur ein paar wenige Schädlinge sind bisher bekannt, einige Distributionen heimgesucht zu haben.

[73] http://sourceforge.net/projects/dsgpl/

8.3 Zugriff über SSH

Eigentlich müsste ich hier schreiben, Zugriff über SSH/Telnet. Doch Telnet ist eines der größten Sicherheitsrisiken beim Fernzugriff, daher möchte ich jeden dringendst dazu auffordern Telnet deaktiviert zu lassen. Durch die Verschlüsselung bei SSH gibt es keine Nachteile. Der einzige Unterschied für Anwender liegt im Port.

Doch genug der Sicherheitsrisiken. Irgendwie lasse ich mich zu oft darüber aus. Sehen wir doch einmal was wir benötigen: Zuerst muss der Zugang im DSM aktiviert werden. Dann benötigen wir noch einen Client. Der berühmteste ist Putty. Dieser ist auch als „portable“-Version verfügbar, sodass man ihn auf einem USB-Stick mit sich herum tragen kann und bei Problemen auf der DiskStation schnell vom nächsten PC aus die Möglichkeit der Wartung hat. Die Konfigurations-Oberfläche sieht aus wie folgt (Screenshot: „Portable“-Version, v. 0.60):



Recht einfach erkennt man hier, dass ich noch keine Adresse eingegeben habe aber Port und Protokoll bereits auf SSH umgestellt sind. Wer nun noch die Adresse seiner DiskStation eingibt (entweder DDNS-Account oder IP-Adresse), kann mit einem Klick auf „Open“ die Sitzung beginnen. Dann dauert es einen Moment bis eine Verbindung steht. Nun sitzen wir vor einem schwarzen Fenster auf dem ein grüner Cursor auf Befehle wartet. Zunächst will Putty die Anmelde-Daten von uns wissen. Man kann sich als „admin“ einloggen oder wenn man tiefer in das System möchte, auf den „root“ zurückgreifen. Sein Passwort ist normalerweise identisch mit dem des „admin“.

Was nun? Zunächst noch einmal der kurze Hinweis: SSH respektive die Shell ist das wohl mächtigste Tool in der gesamten DiskStation. Ein falsches Kommando kann das gesamte System lahm legen.

Wo sind wir eigentlich? Wer sich einen Überblick über das Verzeichnis machen möchte, in dem er gerade arbeitet kann dies mit „dir“ tun. Wem das Verzeichnis nicht gefällt, der kann dies mit „cd“ gefolgt vom Pfad ändern (cd=change directory). Auch das Erstellen eines neuen Ordners gehört noch mit hier hin: „mkdir“ (make directory). Damit sollte man sich erst einmal recht komfortabel bewegen können. Natürlich ist das Wort „komfortabel“ eher vorsichtig zu gebrauchen, denn von unseren grafischen Oberflächen sind wir doch anderes gewohnt und tun uns ein wenig schwer mit dieser Variante.

Wer zum ersten Mal an SSH sitzt wird sich für andere Funktionen viel mehr interessieren, welche dem root vorbehalten sind: Das System-Log „more /var/log/messages“, das Start-Log „dmesg | more“, alle Prozesse „ps -ef“ und alle die derzeit aktiviert sind „top“, das Beenden eines spezifischen Prozesses „killall [Programmname]“, sowie mehr Informationen zur Hardware mit „cat /proc/meminfo“ und „cat /proc/cpuinfo“.

Hinweis: Sämtliche in Klammern geschriebenen Worte müssen ersetzt werden (z.B. „killall httpd“).

Wer sich die Hilfe zu einem Befehl ansieht, dem fällt wahrscheinlich die lange Liste der Angaben auf, welche mit „-" beginnen. Dabei handelt es sich um Optionen, welche in beliebiger Reihenfolge und Menge nach dem eigentlichen Befehl gesetzt werden können. Und wem ein außer Kontrolle geratenes Programm unter die Hände kommt, kann dieses mit der Tastenkombination „Strg+C“ stoppen, allerdings ohne dass dieses vorher ordnungsgemäß beendet wird.

8.3.1 vi

Von vielen gefürchtet, von vielen geliebt. Das ist vi. Dieser Texteditor ist bei allen UNIX-Systemen Standard und sollte daher immer vorhanden sein. So auch auf unserer DS. Doch da wir immer noch von einer Shell reden ist es entsprechend schwierig eine vernünftige Maschine-Nutzer-Schnittstelle zu entwerfen. Denn von einer GUI[74] kann man hier wohl nur eingeschränkt reden. Auch wenn über ipkg Alternativen wie nano zur Verfügung stehen ist vi doch die bessere Wahl insbesondere wenn man nicht nur auf einer DS auf Linux stößt und dann etwas machen möchte.

Am einfachsten ist noch das Öffnen einer Datei. Denn vi ist auch als Kommando verfügbar und lässt sich daher über „vi *Datei+“ aufrufen. Als kleines praxisnahes Beispiel schauen wir uns einmal die Konfiguration des User-Apachen an. Damit wir nichts kaputt machen können kopieren wir zunächst die Originaldatei in ein unser besser zugänglicheres Verzeichnis. Ich setze dabei ein im DSM erstelltes Verzeichnis „Documents“ auf Volumen 1 voraus. Wenn sie ein anderes verwenden möchten tauschen sie bitte den Ordnernamen an den entsprechenden Stellen aus:

cp /usr/syno/apache/conf/httpd.conf-user /volume1/Documents

Nun wechseln wir das Verzeichnis und schauen nach ob die Datei auch angekommen ist:

cd /volume1/Documents

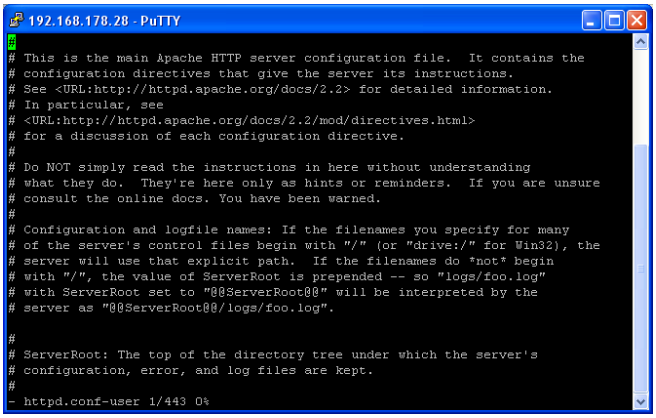
dir

Wenn hier nun die Datei in der angezeigten Liste auftaucht ist alles nach Plan gelaufen. Ab jetzt ist es empfehlenswert nicht als root weiter zu arbeiten um nicht aus Versehen unvorhersehbare Schäden zu verursachen.

Rufen wir einmal die Datei auf und schauen uns an was passiert:

vi httpd.conf-user

Ein relativ spartanisches Fenster mit viel Text und einer kurzen Info am unteren Rand. Na toll. Was lernt man daraus? Wenn man versucht vi selbst zu erlernen steht man hier schnell vor den ersten Problemen, denn anders als bei GUI-Programmen kann man hier nicht einfach ein paar Knöpfe drücken und schauen was passiert.



Also werde ich jetzt mal erläutern was da zu sehen ist. Ganz oben ist ein grüner Cursor der auf Eingaben wartet. Dann folgt der Text wobei die Rauten hier keine Relevanz für vi

[74] GUI = Graphical User Interface, Grafische Benutzeroberfläche

haben sondern von der Konfigurationsdatei als Kommentare dienen. Diese Zeilen werden also später nicht berücksichtigt. Um leere Zeilen zu signalisieren verwendet vi eine Raute (~). Die letzte Zeile enthält den momentanen Status des Cursors, einmal in Angabe „momentane Zeile/Zeilen insgesamt“ und einmal als Prozente.

Da wir uns hier eine Datei ansehen sind wir erst einmal im Kommandomodus. vi kennt den Kommandomodus zur Konfiguration und zum Arbeiten mit der Datei (öffnen, speichern, …) sowie den Eingabemodus zum Editieren des Textes. Wer nun panisch feststellt das vi nichts für ihn ist, der gelangt über die Escape-Taste in den Kommandomodus. Befehle beginnen in vi stets mit einem Doppelpunkt. Sämtliche Eingaben landen jetzt übrigens in der untersten Zeile da ja keine Arbeit am Text als solcher gemacht wird. Das Kommando zum beenden heißt q. Die Eingabe „:q“ beendet also vi und zeigt nun erneut die gewohnte Shell „DiskStation>“ (o.ä.) an.

Wer den ersten Schock überstanden hat und die ersten Tasten drückt stellt schnell fest dass mit den Pfeiltasten im Dokument navigiert werden kann. Um am Text zu arbeiten gibt es je nach Art der Arbeit eine Funktionstaste:

i Vor dem aktuell mit dem Cursor markierten Zeichen einfügen (engl. Insert)
I Am Anfang der momentan markierten Zeile einfügen (kein kleines L sondern ein großes i)
A Hinter dem momentan mit dem Cursor markierten Zeichen einfügen (engl. Append)
A Am Ende aktuellen der Zeile einfügen
o In einer neuen Zeile unterhalb des Cursors einfügen
O In einer neuen Zeile oberhalb des Cursors einfügen

Legen sie diesen Text nun kurz zur Seite und probieren sie ein wenig in der Datei aus. Da wir nur eine kopierte Version editieren ist es auch nicht wichtig was gemacht wird.

Ich möchte jedoch auch hier nur einen kurzen Überblick geben. Das WWW13 bietet genauso viele Informationen zu diesem Thema wie es mittlerweile auch Fachliteratur gibt. Mit den Bild-Pfeil-Tasten ist es möglich auch größere Textpassagen zu überspringen. Doch auch hier stehen wieder weit mehr Befehle zur Verfügung auf die ich nicht eingehen möchte.

Neben dem bereits bekannten :q zum Beenden von vi gibt es noch mehr Optionen. Doch nicht einmal :q wird sie hier befreien, denn wir haben ja etwas verändert aber noch nicht gespeichert. In diesem Fall verlangt vi immer eine gesonderte Bestätigung durch ein Ausrufezeichen. Das Kommando wäre also jetzt :q!

Nicht vergessen: Vorher mit Escape-Taste den Modus wechseln.

Zum Speichern stehen ebenfalls viele Kommandos zur Verfügung von denen ich hier nur wenige nennen werde. Das einfache Speichern erledigt w wie write (engl. Schreiben) welches auch mit Angabe des Zielpfades genutzt werden kann. Um die alte Datei nicht zu überschreiben möchte ich daher lieber die Datei „httpd.conf-user-modified“ speichern. Das entsprechende Kommando lautet:

:w httpd.conf-user-modified

Und fertig ist eine neue Datei.

8.4 / statt C:

Das Linux etwas anders ist, sollten Sie mittlerweile bemerkt haben. Und einen Ansatz hat es von seinen Vorgängern aus der Unix-Welt ganz klar übernommen: Die Anordnung der Verzeichnisse.

Die Grundlage für alles ist nicht wie in Windows ein Laufwerk welches (meist) auch real vorhanden ist, welches Sie also in die Hand nehmen können. Der Ausgangspunkt ist in Linux vielmehr das sogenannte root-Verzeichnis „/“. In dieses hinein werden verschiedene Laufwerke, Ordner etc. hineingesetzt. Eine Festplatte beispielsweise ist in Linux zunächst als eine Art Datei vorhanden welche den Zugang zur Hardware darstellt. Erst das Tool „mount“ bindet nun diese Festplatte real ein. Dieser Vorgang wird daher auch als „mounten“ bezeichnet. Mounten wandelt also ein Stück magnetisches Metall in wirklichen Speicherplatz welcher les- und beschreibbar ist. Kurz gefasst wird dies auch als virtuelles Dateisystem bezeichnet, denn es ist nur virtuell eine Einheit obwohl es eigentlich viele verschiedene physikalische Quellen hat.

Bewegen kann man sich in dieser – für Windows-Anwender ungewohnten Umgebung – mit dem Kommando „cd“[75]. Dessen Funktionsweise möchte ich an zwei Beispielen erläutern:

```
cd /volume1/MeineDaten
```

Dieser Befehl wechselt in den Ordner „volume1“ welcher sich direkt unterhalb des root-Verzeichnisses befindet, und anschließend in den darin befindlichen Ordner „MeineDaten“.

```
cd MeineDaten
```

Hier fällt sofort das Fehlen eines „/“ zu Beginn auf. Das hat zur Folge, dass nun der Ordner „MeineDaten“ nicht mehr direkt unter / liegen muss, sondern auch in dem Ordner in dem man sich gerade befindet liegen kann. Wenn Sie sich also bereits in /volume1 befinden und in den Ordner „MeineDaten“ möchten, so genügt dieser Befehl und Sie müssen nicht den vollen Weg beschreiten wie im ersten Beispiel beschrieben.

Wenn Sie übrigens einen langen Ordnernamen haben, so können Sie die automatische Vervollständigung nutzen. Über die Tabulatortaste laden die meisten Kommandozeilen sofort den Rest des Ordnernamens, sofern es nicht einen anderen Ordner mit ähnlichem Namen gibt.

8.4.1 Die Verzeichnisse des Synology-Linux

Als erstes möchte ich auf den Verzeichnis-Aufbau des Synology-Linux eingehen. Dieser ist nur einsehbar, wenn man sich als „root“ über SSH einloggt. Die Firmware-eigenen Funktionen geben keinen Blick auf die Stammverzeichnisse frei. Aber das zu Recht, denn die kleinsten Änderungen in diesem Teil des Linux können zu großen Problemen, bis hin zu Systemabsturz und Datenverlust, führen.

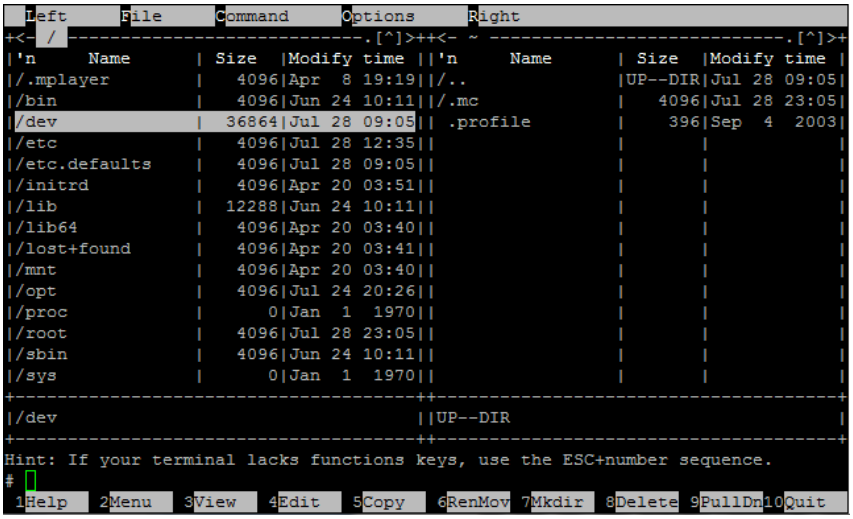
- /bin binaries – In diesem Verzeichnis werden alle Programme gespeichert, die vom Benutzer ausgeführt werden dürfen
- /dev devices – In diesem Ordner werden alle Treiber gepeichert.
- /etc et cetera – Alle wichtigen Konfigurationsdateien werden hier gespeichert.
- /etc.default Die originalen Konfigurationsdateien liegen hier als Backup vor.

[75] „**c**hange **d**irectory“ (Wechsel Verzeichnis)

- /initrd Enthält während des Bootens (Startphase) die Dateien, welche später zur „root-directory“, also „/“ werden. („/“ = Stammverzeichnis, welches ungefähr mit „C:/“ bei Windows-Rechnern vergleichbar ist).
- /lib library – Alle wichtigen Standard-Funktionen der Programme, die häufig verwendet werden, sind in sogenannte Bibliotheken ausgelagert.
- /linuxrc rc=run commands – Datei mit automatisierten Startprogrammen. Dieser Ordner enthält eine Liste, welche Programme während der Startphase ausgeführt werden müssen.
- /lost+found Dieser Ordner wird vom fsck (file-system-check) genutzt, um beschädigte und/oder verwaiste Blöcke (Teile der Festplattenstruktur) zu speichern.
- /mnt mount point – Standardverzeichnis, welches zum temporären „mounten“ genutzt wird. (mounten = Link in einen anderen Ordner / ein anderes Dateisystem unter Linux)
- /opt optional packages – Wird bei der Installation von ipkg angelegt und enthält dessen hinzugeladene Programme/Dateien.
- /proc Dieses Dateisystem, welches eigentlich gar nicht existiert, bietet eine Schnittstelle zu den Kernel- und Prozess-Informationen. Es enthält keine Dateien, stattdessen werden über Befehle wie „cat /proc/meminfo“ Informationen über den Status des Systems abgefragt.
- /root Standardverzeichnis des wichtigsten Benutzerkontos unter Linux (Systemadministrator).
- /sbin system binaries – In diesem Verzeichnis werden alle Programme gespeichert, welche besondere Privilegien erfordern (Systemverwaltung, Dienste, …)
- /sys Ähnlich wie /proc enthält es nur eine Schnittstelle zu den Kernel-Infos.
- /tmp temporary – Temporäre Dateien. Dieses Verzeichnis liegt nicht auf der Festplatte sondern im Arbeitsspeicher. Seine Kapazität ist meist rund 50% des Arbeitsspeichers. Genau wie bei Windows, können Teile jedoch ausgelagert werden um Platz für wichtigere Anwendungen zu machen.
- /usr user – Dies ist das Stammverzeichnis aller anderen Nutzer außer „root“.

8.4.2 Midnight Commander als grafische Alternative

An dieser Stelle möchte ich etwas vorgreifen, denn wie ipkg funktioniert, folgt eigentlich noch. Doch das Tool „mc“ oder Midnight Commander welches via ipkg installiert werden kann, passt einfach zu gut in diesen Abschnitt hinein. Nach der Installation über ipkg erfolgt der Aufruf über ein kurzes „mc“ in der Eingabeaufforderung. Und schon sieht man sich vor einer recht althergekommenen, aber dafür sehr praktischen, grafischen



Oberfläche. Und doch: nach einer Weile kommt einem die Oberfläche recht vertraut vor, denn der Grundaufbau ist auch heute noch meist gegeben. Oben befindet sich eine Reihe ausklappbarer Menüs. Da fällt mir ein dass ich glatt vergessen habe etwas zu erwähnen: mc lässt sich auch mit der Maus bedienen. Unter der Menüleiste ist die Ansicht in zwei Felder getrennt, welche unabhängig voneinander Verzeichnisse darstellen können. Die unterste Leiste sind die wichtigsten Operationen welche sich über die Funktionstasten auf der Tastatur auslösen lassen. Also öffnet sich über die Taste „F1“ auf ihrer Tastatur die Hilfe, über „F2“ das Menü, und so weiter. Sogar ein Editor für einfache Textdateien ist mitgeliefert (Tastaturkürzel ist F4).

8.4.3 Zugriffsrechte

Nachdem jetzt die Navigation etwas besser verständlich sein sollte, wartet noch ein weiterer wichtiger Punkt wenn es um den Zugriff auf Dateien geht. Denn nicht jeder darf alles machen. Dafür gibt es Zugriffsrechte. Und diejenigen die darauf zugreifen dürfen, werden in drei Kategorien eingeteilt: Den Eigentümer der Datei, dessen Gruppe und alle anderen. Der Eigentümer ist neben dem „allmächtigen root“ der einzig befugte um Zugriffsrechte zu ändern. Der Eigentümer hat diese Datei dort abgelegt und kann somit auch über sie bestimmen. Zusätzlich werden die Benutzer in Linux in Gruppen eingeteilt. Nutzer innerhalb einer Gruppe haben meist ähnliche Rechte, weshalb auch hier weitere Rechte eingeräumt werden können. Schließlich bleibt noch der letzte Fall, wenn ein Nutzer zu keiner der vorher genannten Kategorien gehört.

Doch bevor ich Ihnen nun sage wie sie Rechte ändern können, mache ich die aktuellen Berechtigungen erst einmal sichtbar. Das dazugehörige Kommando ist „ls“. Dieses spuckt aber leider recht wenig aus, weshalb es meist mit den Parametern „-al“ aufgerufen wird. Das „a“ blendet auch versteckt Ordner und Dateien ein (beginnend mit einem „.“) und das „l“ listet weitere Informationen wie auch die Berechtigungen. Ein paar typische Zeilen wie sie das Kommando „ls -al" ausspuckt sehen so aus:

```
drwx------    2 root root  4096 Apr 20 03:41 lost+found
drwxr-xr-x    2 root root  4096 Apr 20 03:40 mnt
```

Und schon der jeweils erste Abschnitt ist sehr interessant. Das erste „d“ gibt an, es handelt sich um einen Ordner. Soweit ich spektakulär. Die nächsten Zeichen geben jedoch die Berechtigungen nach dem vorhin genannten Muster an. Zunächst für den Eigentümer, dann dessen Gruppe und zuletzt den Rest der Nutzer. Pro Kategorie können drei Rechte gewährt werden: Lesen (w), Schreiben (r) und Ausführen (x). Ist ein Recht verweigert, so befindet sich stattdessen nur ein einfaches „ – ”. Auf den ersten Ordner im oberen Bild erhält somit dieser Nutzer alle Rechte, jedoch niemand sonst. Auf den zweiten Ordner hat neben ihm auch seine Gruppe das Recht zum Lesen und Ausführen von Dateien und alle anderen können immerhin noch Dateien ausführen. Um nun noch zu erfahren wer denn der Eigentümer der Datei ist (und somit bei Problemen noch schnell Rechte einräumen kann), lohnt ein Blick auf die beiden Namen hinter der Zahl. Im Beispiel handelt es sich also um den Nutzer „root“ in der gleichnamigen Gruppe.

Um Rechte zu ändern, gibt es „chmod“. Dieses Tool ändert über ein Zahlenformat die Rechte an einem Ordner/einer Datei ab. Dieses Zahlenformat ist recht komplex, lässt sich aber in seinen Ansätzen recht einfach erklären. Für ein Recht gibt es genau zwei Zustände: gewährt oder verweigert. Somit liegt schon mal das binäre System mit 0 und 1 auf der Hand. Kombiniert man dies nun noch mit den 3 Möglichkeiten (rwx), so erhält man ein Bit, also eine Zahl von 0-7. Und so setzt sich das Format aus drei Zahlen zusammen. Die erste für den Eigentümer, die zweite für die Gruppe

und die letzte für den Rest. Die Zahl 7 steht beispielsweiße für vollen Zugriff (rwx), die Zahl 6 für Lesen und Schreiben (rw) und die Zahl 4 für Lesen (r). Die anderen Kombinationen sind in der Praxis nur sehr selten vertreten und lassen sich im Notfall nachschlagen. Ein fertiger Befehl sieht also z.B. so aus:

```
chmod 740 log.txt
```

Mit dieser kurzen Zeile würden Sie die Rechte der Datei „log.txt“ also für den Eigentümer auf Voll und für die Gruppe auf Lesen setzen. Alle anderen Nutzer erhielten keinen Zugriff.

Für die Vollständigkeit seien hier auch noch die Befehle für das Ändern von Eigentümer und Gruppe genannt: chown[76] und chgrp[77] nach demselben Muster wie oben (Befehl – neuer Wert – Datei/Ordner). Möchte man sich nur temporär die Rechte eines anderen Nutzers einverleiben, so helfen „su“ und „sudo“. Ersteres wechselt den Benutzer und letzteres führt nur eine einzige Aufforderung unter einem anderen Benutzernamen durch.

8.5 IPKG

Als nächstes möchte ich das IPKG, auch bekannt als „Itsy Package Management System“, ein wenig betrachten. Um das Linux der DiskStation möglichst kompakt zu halten, besitzt das eingebaute Betriebssystem nur die notwendigen Komponenten und Bestandteile. Wer sich jetzt aber mit weiteren Funktionen befassen möchte, kommt kaum am IPKG vorbei. Ursprünglich wurde es für Geräte mit begrenztem Speicher wie Handys oder PDAs erschaffen. Mittlerweile hat es aber seinen Weg auf viele andere Plattformen geschafft. Die eigentliche Aufgabe ist das Installieren und Verwalten von Anwendungen auf Linux-Systemen. Wer beispielsweise openssh installieren möchte, tippt „ipkg install openssh“ in die Konsole (IPKG muss installiert sein). Hat openssh nun seine Arbeit getan und wird nicht mehr benötigt, oder man hat ausversehen das falsche Programm installiert, kann mit „ipkg remove openssh“ wieder die Altlast loswerden. Wer eine vollständige Liste mit allen unterstützten Anwendungen möchte, erhält diese mittels „ipkg list“. Da es sich um eine überwältigende Zahl von verschiedensten Anwendungen handelt, sollte man eher „ipkg list|grep irc“ nutzen. In diesem Beispiel erhält man eine Liste von allen Anwendungen, welche mit IRC (Internet Relay Chat) arbeiten.

8.5.1 Die Installation

Zunächst ist Vorsicht geboten, denn das „Management System“ unterscheidet sich von Prozessor zu Prozessor. Daher sollte man aufpassen, nicht das falsche Paket zu installieren. (Den Prozessor für das eigene Modell findet man bei Synology sowie in unserem Wiki.)

- Für ARM (armv5tejl): http://ipkg.nslu2-linux.org/feeds/optware/syno-x07/cross/unstable/syno-x07-bootstrap_1.2-5_arm.xsh
- Für PowerPC (ppc_6xx): http://ipkg.nslu2-linux.org/feeds/optware/ds101g/cross/unstable/ds101-bootstrap_1.0-4_powerpc.xsh
- Für PowerPC (ppc_85xx): http://ipkg.nslu2-linux.org/feeds/optware/syno-e500/cross/unstable/syno-e500-bootstrap_1.2-5_powerpc.xsh

[76] „change owner“ (Ändere Eigentümer)
[77] „change group“ (Ändere Gruppe)

Nun können Sie mit der Installation beginnen. Zunächst müssen Sie sich als „root“ über SSH einloggen. Nun muss in das Verzeichnis /volume1/public gewechselt werden, wo das Paket zwischengespeichert wird. Anschließend muss der Download gestartet werden. Hierbei müssen Sie unbedingt auf den Prozessortyp achten! Dann muss noch das Skript gestartet und die Liste der zur Verfügung stehenden Pakete gelesen werden.

```
cd /volume1/public
wget http://ipkg.nslu2-linux.org/... (Quelle für Prozessor einfügen)
sh syno-x07-bootstrap_1.2-5_arm.xsh
ipkg update
```

Zum Schluss kann die .xsh-Datei aus dem Ordner „public“ gelöscht werden.

Hinweis: Wer den Ordner „public“ nicht nutzen will, kann einfach ein anderes Verzeichnis als Zwischenablage nutzen. Auch bei den Links sollte man vorsichtig sein, da die Datei durch eine neuere Version ersetzt werden kann. Dann sollte man einfach nachschauen ob es auf dem Server eine ähnliche Datei mit anderer Versionsnummer gibt.

8.5.2 Messung der Übertragungsgeschwindigkeit mittels ipkg-iperf/jperf

Voraussetzungen

- Installiertes ipkg auf der DS und Zugriff via SSH/Telnet inkl. admin-Zugriff und Client (Putty)
- Einen Windows-PC mit aktiver Verbindung zur DS
- Windows-Version von iperf (z.B. von heise.de)

Installation via ipkg auf der DS

Wer ipkg bereits installiert hat sollte recht einfach wissen wie dies zu bewerkstelligen ist:

```
ipkg update
ipkg install iperf
```

Die Installation sollte vollautomatisch erfolgen und keine Fehler anzeigen. Die Bearbeitung von Konfigurationsdateien ist auch nicht notwendig.

Installation auf dem PC

Eine Installation im eigentlichen Sinne ist auf einem Windows-PC nicht notwendig, da iperf als exe vorliegt welche eigenständig lauffähig ist.

Aber: Die fertige Windows-Version ist bei Sourceforge unter "Alle Dateien anzeigen" im Ordner "jperf" zu finden. Das eigentliche iperf-Paket enthält die Quelldateien zum selbst erstellen. Dazu ist allerdings ein gewisses Fachwissen sowie ein Compiler notwendig. Greifen Sie daher lieber zum fertigen "jperf". Das Schöne daran: Sie kriegen gleich ein grafisches Interface mitgeliefert. Wer trotzdem lieber zur Kommandozeilen-Version greifen möchte, der findet diese im Unterordner "bin" als iperf.exe

Den Test vorbereiten: Den Server starten

Und wieder geht es mittels SSH/Telnet auf die DS. Dieses Mal um iperf als Server zu starten. iperf sollte sich nun wie folgt melden:

```
DiskStation> iperf
Usage: iperf [-s|-c host] [options]
Try `iperf --help' for more information.
```

Um iperf zu starten gibt es zwei Möglichkeiten. Die erste wäre als normaler Server, also als ein ganz normaler Prozess, oder als sogenannter Daemon also ein Hintergrunddienst der sich erst meldet sobald er gebraucht wird.

Ein Beispielaufruf als Server:

```
iperf -s -p 4000
```

Die Option -p bestimmt den Port auf welchem iperf mithört.

Nun wartet iperf auf Anfragen von Clienten und vermeldet dies wie folgt:

```
DiskStation> iperf -s -p 4000
------------------------------------------------------------
Server listening on TCP port 4000
TCP window size: 85.3 KByte (default)
------------------------------------------------------------
```

Den Client starten und die letzten Vorbereitungen treffen

Die Java-Anwendung jperf besitzt eine recht aufgeräumte Oberfläche.

Ganz oben sind die wichtigsten Optionen: Adresse und Port des Servers. Viel mehr ist eigentlich nicht notwendig um eine Messung durchzuführen.

Doch ein paar letzte Vorbereitungen müssen noch getroffen werden:

- Alle anderen Anwendungen schließen,
- Sicherstellen das die DS nicht durch andere Prozesse abgelenkt werden kann,
- Alle möglichen Störfaktoren wie Antivierenprogramme und Firewalls deaktivieren.

Der Test

Welche Kommandozeile von der Java-Umgebung genutzt wird, demonstriert die oberste Zeile. Ein Klick auf das linke Symbol auf der rechten oberen Seite des Clients starten den Test. Nun sollten beide beteiligten Seiten anfangen Ergebnisse zu produzieren. jperf stellt diese außerdem in einer Grafik übersichtlich dar.

8.6 Der/Die Apache-Webserver

Die Webserver? Ja richtig! Auf der DiskStation laufen mehr als ein einziger Webserver. Das Problem wäre, dass der DSM Zugriff auf sensible Daten benötigt. Hätte der normale Webserver derartige Berechtigungen, könnte das System sehr einfach infiltriert werden. Da der DSM aber prinzipiell auch „nur“ eine Website ist, benötigt es einen Webserver. Daher läuft neben dem normalen Webserver (/web), welcher unter dem Benutzer „nobody“ (engl. „Niemand“) werkelt, noch eine weitere Instanz, die gewöhnlich System-Apache genannt wird. Diese nutzt die Berechtigungen des root.

Der gewöhnliche Apache, auch „Nutzer-Apache“ genannt, wird erst gestartet, wenn man einen der Prozesse aktiviert, welche gewöhnlich hier laufen: Den Blog, die Photo Station und die Web Station, welche eigene Internetseiten bereitstellt.

Sämtliche Dienste welche über dieselbe Oberfläche laufen wie die Administration, also alles was über den Port 5000/5001 erreicht wird, werden auch dementsprechend vom System-Apache ausgeführt. Dazu zählen neben dem DSM die FileStation, die Audio Station und die Download Station.

9 Linux etwas komplexer

Als Einstand ein Blick auf die Ressourcen. Schließlich kennt man aus der Wirtschaft: Ressourcen sind begrenzt.

9.1 Knappe Resourcen

Zunächst unterteilt Linux den Arbeitsspeicher in zwei in zwei Bereiche: Kernelspace und Userspace. Der Kernelspace ist dem Betriebssystemkern sowie den wichtigen Treibern vorbehalten. Der Userspace wird hingegen von normalen Anwendungen gebraucht welche später gestartet werden. Beide befinden sich natürlich auf demselben Arbeitsspeicher, aber die virtuelle Trennung stellt zum einen die Stabilität des Systems sicher, indem der Kern immer ausreichend Speicher zur Verfügung hat und außerdem wird so der Zugriff auf den Kern reguliert. Ein unbefugter Prozess kann also nicht auf den Kern zugreifen und möglicherweise Schaden anrichten. Doch auch umgekehrt kann der Systemkern nur über große Umwege und unter gewissen Voraussetzungen Daten im Userspace ändern.

Um dieses Konzept noch weiter zu treiben, separiert Linux sogar die einzelnen Anwendungen voneinander. Doch um da nicht die Übersicht zu verlieren, versteckt Linux den wirklichen Arbeitsspeicher vor der Anwendung und schiebt stattdessen eine virtuelle Schicht ein. Programme können also nur auf einen virtuellen Speicher zugreifen, welcher dann den Zugriff auf den echten Arbeitsspeicher regelt und überwacht.

Und doch geht der Platz regelmäßig aus. Für diesen Fall gibt es unter Windows eine „Auslagerungsdatei“. Unter Linux heißt dieses Verfahren swapping und nutzt eine eigene Partition auf der Festplatte. Diese Partition sieht man auch bei Festplatten welche man aus einer DiskStation ausbaut. Doch Linux nimmt diese letzte Option bei hoher Auslastung deutlich seltener in Anspruch als Windows.

Die Arbeit mit der CPU ist weit weniger komplex, denn dort lässt sich weniger regulieren. Linux teilt jedem Prozessor kleine Zeitabschnitte zu in welchem es eigene Berechnungen durchführen darf. Dann ist der nächste Prozess an der Reihe.

Hintergrundprozesse[78] gibt es aber auch bei Linux. Diese werden als Dämon (engl. Daemon) bezeichnet und haben als letzten Buchstaben im Namen meist ein „d“. Diese Prozesse sind also kleine Dauerrenner und verwalten meist Resourcen oder gewähren Zugriff auf Hardware.

Schnittstellen zu Hardware befinden sich unter Linux meist unter /dev und werden, wie bereits besprochen, von Dateien repräsentiert.

9.2 Kernel

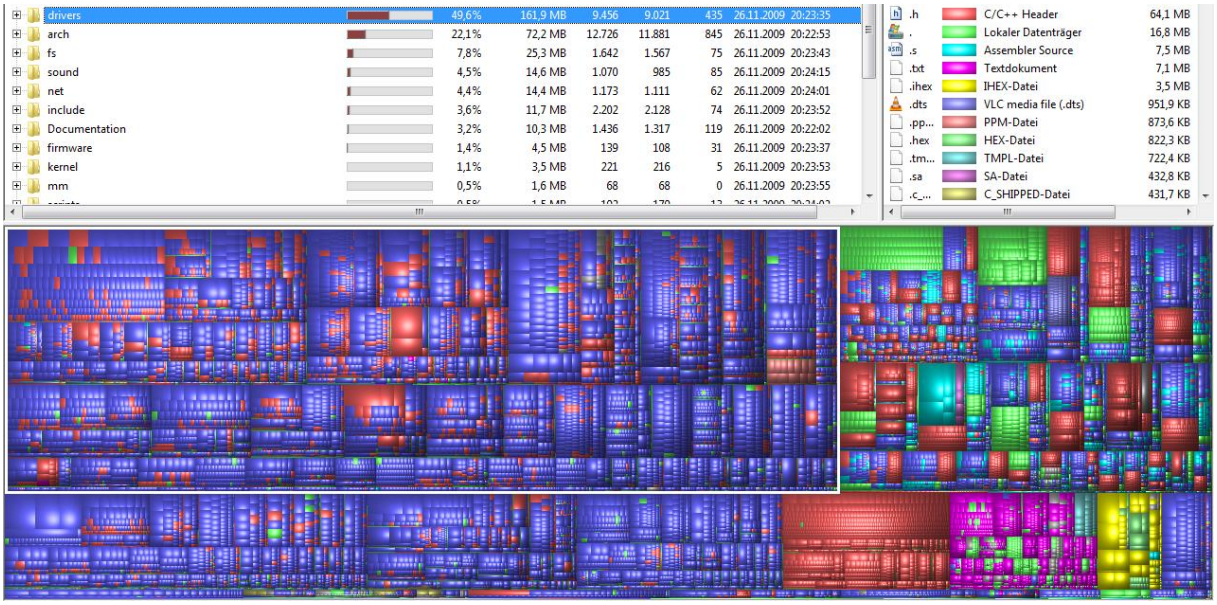
Für die meisten Anwender ist der Kernel der „große graue Klotz, der das System zusammenhält“. In Wahrheit ist er ein faszinierendes Gebilde aus Millionen von Zeilen von Code. Es ist genau die Schicht im laufenden System, welche die Hardware abstrahiert. Das heißt der Entwickler kann recht allgemeine Aufrufe für die Hardware verwenden und egal welcher Treiber dahinter steht, der Kernel übersetzt korrekt. Deswegen ist es Synology auch möglich, verschiedene Hardware-Plattformen zu verwenden ohne für jede eine eigene Firmware zu haben mit unterschiedlichem Funktionsumfang.

[78] Unter Windows auch Dienste genannt

Der Kernel fasst momentan (Version 2.6.30) mehr als 11.5 Millionen Zeilen Quelltext, wird pro Stunde durchschnittlich 6-mal geändert, wächst um fast 13.000 Zeilen pro Tag und an jeder neuen Version arbeiten über 1000 Entwickler mit[79]. Die Entwicklung wird großteilig von der Linux Foundation koordiniert, welche auch einige Entwickler (auch Linus Torvalds) finanziert. Die meisten Entwickler werden jedoch von Sponsoren bezahlt und stehen auch mit diesen offiziell in einem Arbeitsverhältnis.

Doch zurück zur Technik. Unter einem Gesichtspunkt war die Aussage am Anfang dieses Kapitels gar nicht mal so falsch: Der Kernel hält alles zusammen. Er verknüpft Hardware mit Software und Systemprozesse mit installierten Anwendungen. Auch gehen viele der positiven Eigenschaften wie Modularität und Portierbarkeit vom Kernel aus. Wenn man sich die komplexen Zusammenhänge visualisieren möchte, gibt es verschiedene Möglichkeiten der Darstellung. Eine, wie ich finde sehr gelungene, ist hier zu finden: http://www.makelinux.net/kernel_map

Setzt man andere Schwerpunkte, so entsteht ein vollkommen anderes Bild. Ich habe mir einmal den Kernel 2.6.31 runtergeladen[80] und mit WinDirStat[81] eine sogenannte Treemap erstellt:



Der markierte Bereich ist der Ordner „drivers“, also die Treiber. Damit sollte ersichtlich sein, dass der größte Teil des Kernels in der Tat aus Treibern besteht. Der Teil rechts daneben ist der Ordner „arch“, welcher die Anpassung an verschiedene System-Architekturen bewältigt. Darin wiederum macht die „normale“ PC-Architektur übrigens nicht einmal 13% aus (32 und 64-bit zusammen).

Nimmt man all diese Fakten zusammen, so erhält man bei Linux einen monolithischen Kernel. Das heißt auch hardwarebezogene Funktionen wie Treiber sind integriert. Ein solcher Kernel hat jedoch meist das Problem, dass ein einziger fehlerhafter Bestandteil das gesamte System in die Knie zwingt. Linux teilt sich daher in viele Module, welche auch während der Laufzeit neu geladen werden können. Im Gegenzug entfällt die sonst schwierige und angreifbare Kommunikation zwischen Kernel-Bestandteilen wie bei anderen Alternativen üblich. Auch kann die Resourcenverwaltung so direkt

[79] Quelle: „Linux Kernel Development“, The Linux Foundation (http://www.linuxfoundation.org/sites/main/files/publications/whowriteslinux.pdf)
[80] Offizielle Internetseite des Linux-Kernels: http://kernel.org/
[81] http://windirstat.info/

zwischen Systembestandteilen und Nutzeranwendungen unterscheiden und entsprechende Prioritäten setzen.

Wenn man aber ein Betriebssystem, beispielsweise für ein NAS schreibt, so kann man den Kernel stark verkleinern indem man die Unterstützung für andere Architekturen sowie die Treiber für nicht benötigte Hardware wie Grafik einfach entfernt. Doch gerade für letzteres ist viel Erfahrung und Arbeit nötig.

9.3 Kommandozeile

Ich rede gern von der Kommandozeile, wohlwissend dass es „die Kommandozeile“ eigentlich nicht gibt. Denn auch diese ist eine Anwendung wie ein grafischer Desktop wo es viele verschiedene Alternativen gibt. Daher ist es manchmal wichtig zu wissen, dass es bei manchen Systemen Unterschiede gibt. Und der Teufel liegt meist im Detail.

Eigentlich ist der Begriff Kommandozeile falsch, denn das Programm interpretiert eine Eingabe welche ich in Textform tätige. Daher findet man häufig den Begriff „Kommandointerpreter“. Doch genug der Theorie

Angefangen hat alles in den 70er Jahren mit der Bourne-Shell, welche auch „sh“ genannt wird. Da die Möglichkeiten damals aber gering und der Syntax kompliziert blieb, erarbeitete man die C-Shell, welche sich an die Programmiersprache C anlehnt und somit den meisten Entwicklern leichter von der Hand geht. Mit der Korn-Shell ging man erstmals einen Zwischenweg. Basierend auf der Bourne-Shell übernimmt sie dennoch viele der Vorteile der C-Shell (ksh).

1987 kommt mit der Bourne-Again-Shell oder kurz bash der heute größte Vertreter ans Tageslicht. In späterer Zeit folgen noch u.a. „tcsh“ (TC-Shell) sowie „zsh“ (Z-Shell).

Doch egal mit welcher man sich normal beschäftigt, das Programm chsh (change shell) wechselt die einem Nutzer zugewiesene Shell problemlos. Nach einer neuen Anmeldung sieht man sich anschließend auf der neuen Shell wieder.

Unter Prompt bezeichnet man in diesem Zusammenhang das, was bereits vor jeder Eingabe in der Zeile steht. Es ist also die Aufforderung zur Eingabe. Bei einigen Shell-Systemen sieht man da beispielsweise „user$“, bei einer DiskStation „DiskStation>“. Bei den meisten Systemen ist diese kurze Phrase auch änderbar.

Beschäftigt man sich etwas genauer mit der Shell, so muss man zwischen „Built-in“ und „Programm“ unterscheiden. Über eine Shell lassen sich ja wie bereits gesehen Programme starten. Doch einige Kommandos sind auch in die Shell einprogrammiert und werden daher als „eingebaut“ bezeichnet. Doch genau diese können sich zwischen den Shell-Arten unterscheiden, sowohl in Handhabung als auch im Funktionsumfang.

Für alle, die sich etwas näher mit der Kommandozeile beschäftigen möchten, kann ich nur die Shell-Programmierung empfehlen, für alle anderen sollte dies an Informationen vorerst genügen.

9.4 Systemadministration

Eigentlich gehören zu einem Betriebssystem noch viel mehr Aufgaben. Da wären zum Beispiel verschiedene Benutzer welche verwaltet werden möchten. Oder Dienste welche starten und stoppen, je nach Bedarf. Da Synology all diese Funktionen jedoch angepasst hat um alle

Anwendungen zu erreichen und die Administration über den DSM zu ermöglichen, gibt es auf der Kommandozeile eigene Anwendungen.

Um Nutzer hinzuzufügen gibt es auf Linux-Systemen die Funktion useradd, welche sich über viele Optionen bis ins Detail steuern lässt. Eine Schritt-für-Schritt-Alternative bietet das Tool adduser, welches jedoch von der Distribution abhängig ist bzw. bei einigen ganz fehlt. Synology hat alle Funktionen zum Verwalten der Nutzer in das Programm „synouser“ gepackt. Über die Option „-add“ lassen sich neue hinzufügen. deluser bzw. userdel dient hingegen dem Löschen von Nutzern. Bei Synology geschieht dies über das gleiche Modul jedoch mit dem Anhang „-del“. Die Gruppenverwaltung hat Linux in die Datei „/etc/group“ ausgelagert. Synology steuert dies hingegen wieder über ein Programm, nämlich „synogroup". Einzig das Hinzufügen von Nutzern zu Gruppen lässt sich unter Linux über ein Kommando erreichen: „adduser [Nutzer] [Gruppe]“.

Auch die Verwaltung von Software gehört unter Linux zu den Standardaufgaben eines Administrators. Auf einer DiskStation gibt es dafür ipkg, doch in der Desktop-Welt gibt es andere Systeme. Eines ist das Debian-Paketsystem (Endung .deb), welches sich über „dpkg“ oder „apt-get“ steuern lässt. Ersteres ist jedoch mehr für Hobby-Masochisten und Vollblut-Administratoren. Auf vielen Distributionen ist außerdem „aptitude“ mitgeliefert, welches eine grafische Oberfläche auf Textbasis bereitstellt. Ebenfalls sehr beliebt ist das RedHat-System, welches mit sogenannten RPMs arbeitet (Dateiendung .rpm). Das klassische Verwaltungstool heißt daher auch ganz schlicht „rpm“. Um noch ein letztes zu nennen bliebe das Slackware-System. Es besitzt die Kernkomponenten „installpkg“, „removepkg“ und „upgradepkg“. Die textbasierte Verwaltung heißt „pkgtool“.

Doch auch da hört die Arbeit eines Admins nicht auf. Da wären zum Beispiel noch die Backups. Hierzu kann man entweder spezielle Backuptools nehmen wie rsync (in diesem Fall auch noch zugeschnitten auf Netzwerke) oder man sichert die gesamte Festplatte mit „dd“. Doch auch ein normales Archiv mit „tar“ sichert Daten zuverlässig (evtl. noch mit Komprimierung wie „gzip“). Aber weil man mit diesem Thema alleine ganze Bücher füllen kann, werde ich mich damit nicht weiter beschäftigen.

Ich bin mir bewusst, dass es eigentlich noch viel mehr gibt. Doch ich möchte das Thema Administration bewusst kurz halten. Selbst wenn Sie sich irgendwann für ein Desktop-Linux entscheiden, so gibt es für alle hier beschriebenen Aufgaben grafische Tools und Sie werden nur sehr selten in die Verlegenheit kommen, die Kommandozeile für eine der hier vorgestellten Aufgaben zu nutzen.

9.5 Berechtigungen Teil 2: Access Control Lists

Ich hatte bei den Firmware-Funktionen schon mal die Windows-ACLs aufgegriffen. Denn genau die unterstützt eine DiskStation seit Firmware 3.0. Doch auch darunter verbirgt sich eine Technologie die Linux nicht fremd ist. Nur lassen sich diese ACLs über Linux-PCs noch nicht editieren, daher die Benennung des Features.

Und wenn Sie sich nicht sofort wieder erinnern so sei noch einmal gesagt: ACLs treiben die Rechteverwaltung auf die Spitze, sodass man für jeden Nutzer und jede Gruppe einzeln Rechte für Dateien und Ordner festlegen kann (und nicht nur für Eigentümer, Gruppe und den Rest).

Über die Kommandozeile gibt es da ein Tool namens „setfacl“, aber das ist eine Wissenschaft für sich. Hervorzuheben ist aber: Die alten Rechteeinstellungen existieren noch und werden auch noch genutzt! Wenn der Nutzer der Eigentümer ist, so gelten nach wie vor die alten Gesetzmäßigkeiten.

Erst dann treten die ACLs in Aktion. Und jetzt gilt: Die genaueste Regel gilt! Wenn es also einen Eintrag für einen Nutzer und dessen Gruppe gibt, so gilt der explizite Eintrag für den Nutzer. Stehen aber wiederum die „alten“ Rechte mit den ACLs im Konflikt, so haben die herkömmlichen Vorrang. Abgerufen werden können die ACLs über „getfacl“.

9.6 Immer wieder dasselbe: cronjobs

Möchten Sie alle 10 Minuten zum PC laufen um ihm zu sagen, er solle bitte ein kurzes Backup durchführen? Belastend, oder? Daher gehört die regelmäßige Ausführung von Programmen zum Standardumfang eines jeden Betriebssystems. So gibt es unter Linux die cronjobs. Genauer genommen gibt es den Prozess „crond“ welcher bei Bedarf aktiv wird (cron daemon). Festgelegt werden die Abläufe in „Crontab“ einer Art Stundenplan welcher aus einer einfachen Textdatei besteht. Die verschiedenen Spalten werden dabei über Tabulatoren-Sprünge festgelegt.

Eine solche „crontab“ könnte beispielsweise so aussehen:

#minute	hour	mday	month	wday	who	command
0	0	*	*	*	root	/usr/sbin/ntpdate -b pool.ntp.org
0	1	*	*	1,4	root	/usr/syno/bin/synolocalbkp -a

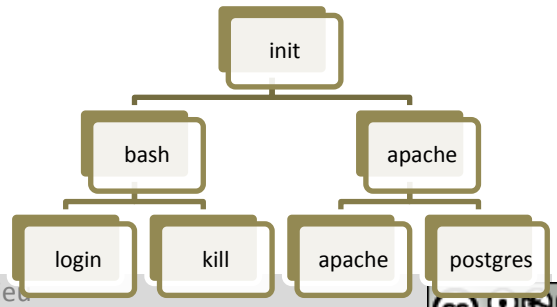
In der ersten Spalte wird angegeben, zu welcher Minute der Befehl ausgeführt werden soll. Steht dabei „*/5“ so wird der Befehl alle 5 Minuten ausgeführt, daher das „*/“. Wird hingegen jede Minute der Befehl benötigt, so gibt es noch die Möglichkeit eines einfachen „*“. Ähnlich sehen dann auch die weiteren Spalten aus. Die nächste Spalte enthält Angaben über die Stunde, die nächste über den Tag (1-31), dann der Monat und schließlich der Wochentag, wobei Sonntag hier dem Wert 0 und dem Wert 7 entspricht.

Als letztes wird noch angegeben unter welchem Nutzer dies ausgeführt und was genau gemacht werden soll. Dabei ist ein Kommando erlaubt, genauso wie Sie es auf der Kommandozeile direkt angeben können. Soll es aber komplexer sein, müssen Sie ein Shell-Skript schreiben und auf dieses angeben. Wichtig ist aber zu jeder Zeit die Angabe der vollen Pfade um Probleme zu vermeiden. Theoretisch geht es bei einigen auch ohne. Theoretisch!

9.7 Prozesse

Ein Programm ist eine Datei welche ausgeführt werden kann. Dadurch entsteht schließlich ein Prozess oder sogar mehrere. Diesen Unterschied muss man sich klar machen, denn nur ein Prozess verrichtet eigentlich Arbeit. Jeder Prozess hat unter Linux eine eigene Nummer, die PID. Über diesen lässt er sich gezielt ansteuern, denn sie ist einmalig, wird jedoch erst zur Laufzeit vergeben und ist somit nicht immer identisch mit der vom letzten Mal.

Doch die Welt der Prozesse ist klar geregelt, denn es herrscht eine Hierarchie an dessen Spitze der Prozess „init“ steht, welcher beim Booten vom Kernel erzeugt wird. Er ist also der Adam aller Prozesse, denn alle anderen sind seine child-Prozesse, also wortwörtlich übersetzt Kinder. Dieser Prozess wird als „forking“ bezeichnet. Beim *forken* werden dabei gewisse Informationen über die Umgebung mitgegeben, wie beispielsweise gewisse Pfade zu wichtigen Dateien. Es entsteht somit eine baumartige Struktur. Wird nun ein Prozess beendet, so müssen auch alle Child-Prozesse stoppen. Geht



dabei etwas daneben, so heißt der nun „verwaiste“ Prozess Zombie. Hierbei handelt es sich meist um Programmierfehler. Eine Baumansicht lässt sich mit „pstree“ aufrufen.

Ein Prozess kann aber auch schlafen. Er hat also momentan keine Arbeit, wartet aber auf ein Signal von außen um daraufhin wieder in den Zustand „laufend“ zu wechseln. Möchte man nun einen fehlerhaften Prozess wie einen Zombie loswerden, so muss er aus dem Arbeitsspeicher entfernt werden. Dazu dient das Kommando „kill“ mit angehängter PID. Die PID lässt sich über die Ausgabe von „ps“ bzw. „ps –A“ auslesen. Alternativ gibt es das Programm killall, welches jedoch bei gleichen Namen (was bei Linux problemlos möglich ist) alle Prozesse schließt. Tippt man auf einer DiskStation beispielsweise „killall httpd“ hat man ein Problem, denn alle Webserver inkl. der Administrationsoberfläche sind damit nicht mehr erreichbar.

kill kann jedoch deutlich mehr als nur Prozesse beenden, denn eigentlich übersendet es kurze Signale. Das zum Beenden hat dabei die Nummer 9, wird jedoch immer angewendet wenn kein weiteres genannt wurde. Über „kill -19 rsync“ lässt sich aber auch das Backup anhalten. 19 steht für „STOP“, 18 für „CONT“ (Continue=Fortsetzen). Ein Neustart wird über 1 erzwungen.

Um möglichst effektiv zu arbeiten muss der Kernel Prioritäten setzen. Das entsprechende Kommando lautet „nice“ um die Priorität herabzusetzen. Erhöhen ist nur dem Administrator (root) möglich. Die höchste Priorität ist mit dem Zahlenwert „-20“ verbunden, die geringste mit „19“. Man ist also nett, wenn man über die Option „-n“ zu „nice“ auf Rechenzeit verzichtet. Zum freien Verändern bei bereits laufenden Prozessen eignet sich „renice +5 -p 12“. Dabei wird hier die Priorität PID 12 um 5 herabgesetzt (also der Zahlenwert um 5 erhöht). Mehr Rechenleistung gewinnt man jedoch nicht, denn diese wird nur anders verteilt als bisher.

Doch wer Linux nun auf dem Desktop nutzen möchte, muss sich nun zunächst eine Distribution aussuchen. Beliebt sind dabei u.a. Ubuntu, openSUSE und Fedora, doch die Entscheidung bleibt letztendlich eine sehr persönliche, welcher jeder für sich anders entscheiden wird.

10 Einführung in html und PHP

Um den Webserver vernünftig nutzen zu können, kommt man häufig nicht um ein wenig Grundwissen zu html und PHP herum. Dass insbesondere html aber keine Wissenschaft ist und auch ohne vorherige Programmierkenntnisse zu bewältigen ist, werde ich gern beweisen.

10.1 html

html ist die Urform des Webs. Tim Berners Lee schrieb am CERN den ersten Webserver und ersten Browser – beides sollte mittels html kommunizieren. Da er damit das Web erschuf, hat er auch viele Auszeichnungen dafür erhalten.

Aber ohne viel mehr Vorreden möchte ich direkt einsteigen, denn html ist nicht so kompliziert das man dafür viel einleitende Worte verlieren müsste:

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
          <head>
          </head>
          <body>
                    Hallo Welt!
          </body>
</html>
```

Dieser „Mindestaufbau“ enthält alles um ein wenig Text darzustellen. Die erste Zeile legt fest, welche html-Version verwendet wird. Ist diese Zeile nicht vorhanden, kann der Browser in einen anderen Modus schalten um möglichst viel darzustellen. Da er aber nicht genau weiß, welche Dateiform er empfangen hat, kann er nur mit Annahmen arbeiten.

Anschließend wird über den Tag „<html>“ der in html programmierbare Teil begonnen. Ab hier werden immer Tags ineinander verschachtelt: Der Beginn wird über „<Tag>“ festgelegt, das Ende über „</Tag>“. Nur einige Tags kommen auch ohne Ende aus. Werden Tags ineinander verschachtelt, so gehört es zum guten Programmierstil diesen Aufbau über Einrückungen zu kennzeichnen.

Hier mal noch eine Reihe der beliebtesten html-Tags:

Eröffnungs-Tag	End-Tag	Auswirkung	Beispiel
<h1>	</h1>	Überschrift – je größer die Zahl, desto „untergeordneter“	Dies ist die Überschrift
<h1 align=“center“>	</h1>	Wie oben, nur jetzt zentriert dargestellt. Auch möglich: left, right, justify (Blocksatz)	<h1 align=“right“> Rechtsbündige Überschrift </h1>
** **		Absatz	Dies ist ein Absatz mit viel Text
** **		Einfacher Zeilenumbruch	Erste Zeile Zweite Zeile
****		Fett geschriebenen Text (für kursiv: i, unterstrichen: u)	Das ist FETT
** **		Text zentrieren	Zentriert
****		Hyperlink zu example.org	Deutsches Synology-Forum
<img src=”example.org/ bild.gif”>		Bild einblenden (Urheberrecht beachten!), kombinierbar mit align	<img src=“http://www.synology-forum.de/index.html“>

Wer sich noch näher damit befassen möchte, sollte sich auch CSS ansehen, welches Styles definieren kann.

Ansonsten werde ich hier mit html aufhören, da es wirklich nicht viel mehr zu sagen gibt wenn man einen kurzen Überblick geben möchte. Basierend auf dem einfachen Baukastenprinzip lässt sich dieser Code recht schnell schreiben und lesen. Wer wissen möchte was mit html noch möglich ist (insbesondere html5 bringt neue Möglichkeiten mit sich, u.a. in der Integration von Multimediainhalten), der kann sich dazu zahlreich an anderen Stellen belesen.

Heutzutage wird übrigens nur noch selten html von Hand geschrieben – sogenannte „IDEs“ (Plattformen, die alles für Entwicklungen notwendige mitbringen und Routinearbeiten automatisieren) fertigen diese Grundgerüste sofort an; und für reine html-Seiten werden grafische Editoren wie „KompoZer“[82] verwendet.

10.2 PHP

PHP ist verglichen mit PHP deutlich „dynamischer“. Zunächst hat man die Wahl, eine Datei „.php“ zu nennen oder „.html“. In beide lässt sich PHP bei entsprechend konfiguriertem Webserver einarbeiten. Dazu dient ein Tag wie oben erläutert, welcher jedoch aufgebrochen wird: <?php … ?>.

Innerhalb dieses Kastens können beliebig viele Anweisungen, mit „;“ getrennt, aufgeführt werden. PHP lehnt sich in seiner Struktur an die meisten anderen Programmiersprachen an. Wer also schon eine solche (am besten C) beherrscht, wird sehr schnell erste Erfolgserlebnisse haben.

Variablen müssen in PHP aber nicht initialisiert werden. Sie beginnen mit einem „$“ gefolgt von (mindestens einem) Buchstaben. Variablen, welche mit „$_“ beginnen, sind vom System vorbelegt. Etwa „$_GET[]“, welches einen Parameter aus der URL (mit ? angehängt) abruft.

Ein Beispiel: (aufgerufen: index.php?index=1)

```
<?php
$variable = „Das wird Text“;
$variable = „und jetzt hab ich sie überschrieben“;
$321 = „das hier wird eine Fehlermeldung geben …“;
$variable = $_GET[index];
echo $variable;
$>
```

Als Ausgabe wird „1“ erscheinen, den mit „$_GET[index]“ wird der hinter „index.php“ übergebene Parameter „index“ abgerufen und mit „echo …“ wird dieser Wert anschließend ausgegeben. Es kann auch html-Code ausgegeben werden, der anschließend vom Browser korrekt interpretiert wird.

Für die meisten Prozeduren wie „if“ werden statt „begin“ und „end“ "{" und "}" verwendet. Zuweisungen erfolgen über ein schlichtes „=“, ein Überprüfung auf Gleichheit, etwa bei „if“, über „==“.

Ein paar Beispiele:

```
<?php
$variable = „Text“
if ($variable == „Text“)
          echo „Es funktioniert“;
if ($variable == „Anderer Text“
```

[82] Webseite: http://kompozer.net/

```
$>
```

Eine Datenbank kann mittels mysql bzw. mysqli eingebunden werden. Dafür ist aber wiederum die MySQL-Sprache notwendig, was nicht immer einfach ist, auch wenn man damit sehr viel und komplex arbeiten kann.

Soviel zur kurzen Einführung. Damit sollte das nächste Kapitel „CMS4DS“ auch für Laien etwas verständlicher sein.

Bild: Unter (cc)-Lizenz von „depone“ („Flickr“)

11 CMS4DS

11.1 Wozu ein neues CMS?

Wer auf seiner DiskStation ein umfangreicheres Web-Projekt laufen lassen möchte, der wird mit sehr hoher Wahrscheinlichkeit schon einmal über sogenannte CMS gestolpert sein. Ein „Content-Management-System“ verwaltet, wie der Name schon sagt, den gesamten Inhalt (Content) eines Web-Projektes selbstständig über eine eigene Verwaltungsseite. Gibt man nun mal bei Google „CMS“ ein, wird man hunderte von verschiedenen Systemen finden. Die Schwerpunkte liegen dabei sehr unterschiedlich. Während Wordpress beispielsweise ursprünglich als reine Blogsoftware entwickelt wurde, ist es zu einem der beliebtesten CMS und dem wahrscheinlich am weitest verbreiteten Blogsystem geworden. Joomla hingegen ist ein Universalwerkzeug um eine eigene Webpräsenz zu erstellen. Sowohl Wordpress als auch Joomla können durch eine Vielzahl von Plugins, welche von jeweils riesigen Communities entwickelt und bereitgestellt werden, mit fast allen nur denkbaren Funktionen ausgestattet werden.

Doch damit wäre immer noch nicht geklärt, warum itari fleißig an einem eigenen CMS arbeitet. Eigentlich ist der Markt für derartige Software doch gesättigt, sollte man meinen. Doch nun zum Haken: Da die CMS eine Unmenge von verschiedensten Informationen sammeln und bereitstellen müssen, gibt es für die Entwickler meist nur eine Lösung: PHP und SQL. Wie wir bereits gesehen haben, muss SQL zunächst von PHP aufgerufen werden und das Ergebnis dann in html umgewandelt werden, bevor die Seite sich auf die Reise machen kann. Solange die CMS auf einem typischen Webserver laufen, also einer oft mehrere Tausend Euro teuren Hochleistungsmaschine, stellt das kein Problem dar. Nun besitzt unsere DiskStation aber weniger Rechenleistung als ein normaler Heim-PC (ist dafür aber sicherer, billiger, sparsamer und zuverlässiger). Aus Spaß oder zum Testen kann man gerne mal ein CMS auf der DiskStation installieren. Gerade wenn man kein „+“-Modell hat, sollte das Ergebnis allerdings nicht wirklich zufriedenstellend sein. Die Ladezeiten können dabei schnell viele Sekunden betragen. Es kann auch sein, dass von außen (Internet) aufgrund zu langer Ladezeiten die Anfrage abgebrochen wird und der Nutzer dann eine Fehlermeldung vor die Nase gesetzt bekommt.

Ich denke ich habe nun das Problem ausreichend dargestellt. Sehen wir einmal was itari dagegen unternommen hat.

11.2 Das Konzept

Wer jetzt dachte, er hätte ein tolles CMS für seinen kleinen Wunderkasten gefunden, welches man einfach mit ein paar Klicks installieren kann, den muss ich leider enttäuschen. Itari möchte nicht nur ein schnelles CMS bereitstellen, sondern auch dass wir ein wenig über Web-Programmierung lernen.

So besitzt das CMS4DS weder eine fertige Installationsroutine, noch eine einfache Möglichkeit alles im Blick zu behalten, geschweige denn ein festes Design. Außerdem ist das Grundkonzept auch nicht an eine Datenbank angebunden. Man muss sich daher ein wenig mit dem Aufbau einer Website sowie PHP und html auskennen. Auch weiterführende Kenntnisse zu SQL-Anbindung sind empfehlenswert, wenn man die Funktionalität ausbauen möchte. Ich werde trotzdem versuchen es so einfach wie möglich zu erklären, sodass man auch mit wenig Wissen über diese Gebiete etwas erreichen kann.

Bevor Ich beginne, noch ein wenig zu den Prinzipien hinter diesem CMS. Es sollte so wenig wie möglich PHP und anderen Server-seitigen Code besitzen. Gegen JavaScript und andere Client-basierte Sprachen spricht dagegen nichts. Wer will kann mit JavaScript ein Feuerwerk von Effekten auslösen, solange er so wenig wie möglich PHP dabei einsetzt. So kann sichergestellt werden, dass unser cms4ds das bleibt, wofür es geschaffen wurde: schnell. Des weiteren ist bei Browser-Weichen Vorsicht geboten. Also bei Code, der von Browsern unterschiedlich interpretiert wird oder den manche gleich gar nicht verstehen. Die Grundlagen wie Ich sie hier besprechen werde, laufen mindestens mit Firefox und Internet Explorer ohne Probleme.

Trotz des Namens ist das cms4ds am Ende halt „nur“ eine umfangreiche Internetseite. Daher läuft es nicht nur auf einer DS sondern auf jedem Server, der PHP5 und eventuell eine Datenbank bereitstellt. Das trifft meist auch auf bezahlten Webspace zu. Bei kostenlosen Hostern ist es aber eher die Ausnahme. Da es keine weiteren Änderungen am Linux benötigt, ist es außerdem keine 3rd-Party-Application sondern eine „einfache“ Webanwendung wie sie Synology selbst auf der eigenen Internetseite listet.

11.3 Der Aufbau

Nun geht es ans Eingemachte. html-Dateien besitzen im cms4ds nur eine kleinere Rolle: sie besitzen die Verweise zu den verschiedenen Bestandteilen wie dem header und footer (Kopfelemente und Fußleiste). Der wichtigste Teil gestaltet sich dabei wie folgt:

```
<!--#include virtual="header.html" -->
<!--#include virtual="cms4ds.php?where=cms4ds" -->
<!--#include virtual="footer.html" -->
<script>LoadRSS2("http://www.synology-forum.de/external.html?count=12");</script>
<!--#include virtual="bottom.html" -->
```

Schritt für Schritt:

In der ersten Zeile wird der header, also die Überschrift und das kleine Bild sowie das Menü am oberen Rand, eingebaut.

Die zweite Zeile lädt eine PHP-Datei, welche den gesamten dynamischen Inhalt lädt. Über die Angabe „?where=“ wird die Position per Variable übergeben. Diese Variable ist von Seite zu Seite unterschiedlich.

Die dritte Zeile enthält den sogenannten footer. Er enthält den Hinweis des Copyrights sowie ein paar kleine Zahlen, wie lange der Aufruf gedauert hat.

Als nächstes wird der blaue Kasten am rechten oberen Rand gefüllt. Itari nutzt dabei einen von unserem Forum bereitgestellten RSS-Feed.

Die letzte Zeile, die bottom.html, lädt im Hintergrund alle Unterseiten vor, zeigt zunächst aber nur die erste an. Alle anderen zeigt es in einer kleinen Liste rechts unten an.

11.4 Die html-Seiten im Detail

Jetzt kommen wir zur genauen Funktion der einzelnen Dateien, von denen Sie bisher nur gesehen haben was sie machen sollen.

11.4.1 Header.html

Oben haben wir gesagt, dass der header sich mit der Überschrift, dem Kopfbild und dem Menü befasst.

```
<!--#set var="t" value="" -->
<html><head><title>cms4ds</title>
<link rel="stylesheet" type="text/css" href="cms4ds.css" />
<link rel="alternate"  type="application/rss+xml"
                       title="cms4ds-News-Feed" href="cms4ds_rss.php"/>
<link rel="shortcut icon" href="cms4ds.ico" />
<link rel="search" type="application/opensearchdescription+xml"
      href="http://syno/cms4ds/search.xml" title="cms4ds" />
<script type="text/javascript" src="cms4ds.js"></script>
<script>var d0,d1,d2,d3;d0=new Date().getTime();</script>
</head><body onload="history()">
<iframe src="blank.html?0" name="histFrame" id="histFrame"></iframe>
<div id="basecontainer">
<div id="top">cms4ds<br/><span>a CMS for Synology Disk Stations</span></div>
<div id="menu">
<a href="cms4ds.html">cms4ds</a>
<a href="files.html">files</a>
<a href="stylesheet.html">stylesheet</a>
<a href="javascript.html">javascript</a>
<a href="database.html">database</a>
<a href="rss.html">rss</a>
<a href="search.html">search</a>
<a href="tools.html">tools</a>
</div> <!-- menu -->
<div id="container">
<div id="container_col">
<input id="search" ondblclick="searchAll(this.value)"
       title="Doppelklick zum Starten des Suchvorgangs"
       value="(Suchbegriff)"/>
<div id="counter"># Besucher</div>
<div id="feed"></div>
<div id="index"></div>
</div> <!-- container_col -->
<div id="content">
```

Genau genommen macht er aber noch viel mehr. Im ersten Teil wird die CSS-Datei, welche das Aussehen vorgibt und der RSS-Feed, verlinkt. Außerdem wird der Dateiname des kleinen Mini-Bildes für den Browser definiert. Außerdem bieten ja bekanntlich verschiede Browser kleine Suchleisten an, die einem das Eintippen der Suchseite erspart. Damit auch unsere Seite entsprechend genutzt werden kann, wird die xml-Datei verlinkt welche dafür verantwortlich ist.

Die nächsten Zeilen sind besonders wichtig. Die größten und wichtigsten Funktionen werden nämlich per JavaScript abgewickelt, da sie das CMS schlank halten. Der entsprechende Link befindet sich in diesen Zeilen. Was genau dort passiert, werden wir später sehen.

Mit dem Beginn des eigentlich sichtbaren Teils (<body>) wird die Funktion „history“ ins Leben gerufen. Das ganze läuft über einen iframe. Mit einem iframe kann man einen gewissen Bereich von einer anderen html-Datei einbinden. Das einzig wirklich wichtige für uns ist, dass die „blank.html“ vorhanden ist, damit wir nicht das Risiko eines Fehlers bei manchen Browsern eingehen.

Um den Rest des Textes ein wenig kurz zu halten: Es wird der Kopf mit Überschrift und Bild sowie das Menü eingefügt. Um für das Menü nicht noch gleich ein paar mehr Skripte zu verbrauchen, werden gleich die Links mit eingefügt (die lange Liste <a href…). Außerdem wird die Struktur des rechten Kastens vorbereitet. Der Inhalt kommt, wie fast überall, von einer externen Quelle.

Nur der Vollständigkeit halber: Alle weiteren nötigen Informationen kommen von einer CSS-Datei. Itaris Hauptgedanke dahinter ist, Inhalt und Design so klar wie möglich zu trennen.

11.4.2 footer.html

```
</div> <!-- content -->
</div> <!-- container -->
<div id="footer">(c) 2008 by &#x81F3; itari based on cms4ds</div>
<div id="timer"><!--#echo var="t" --> # </div>
</div> <!-- basecontainer -->
```

Der „footer“ enthält die untersten zwei Zeilen des CMS. Die erste beinhaltet den Copyright-Hinweis (Quelltext Zeile 3) und die zweite die gemessenen Zeiten, wie lange es gedauert hat um die Seite zu laden.

11.4.3 bottom.html

```
<script>
make_index();
s=window.location.search; if (s.substr(1,1)=='s') searchAll(s.substr(3));
if (s) showme(s);
</script>
</body></html>
```

Obwohl diese Datei kurz ist, stellt sie einen wichtigen Teil dar. Auch für uns wichtig zu wissen ist, dass die Funktion „make_index“ alle **Überschriften mit h3-Markierung** heraussucht und dann als **Überschriften für die Beiträge**, deren Liste rechts unten angezeigt wird, festlegt. Außerdem wird die Eigenschaft „display“ aller anderen Beiträge wird auf „none“ gesetzt, damit sie unsichtbar werden und erst dann erscheinen, wenn man sie gerne hätte.

Noch als letzter Hinweis: Sie sollten darauf achten, dass alle Ordner mit .htaccess ausreichend abgesichert sind! Der Download von itari bringt schon ein paar mit, doch die treffen nicht für jeden Einsatzzweck zu. Außerdem schalten sie die SSI[83] ein. Mehr zu htaccess folgt in Kapitel 12.

11.5 Stylesheet

Mit den html-Dateien haben wir zwar die Grundsteine gelegt um Inhalt wiederzugeben, doch bisher fehlt jegliche Aufteilung der Elemente, eine Definierung der Schriftart, Farben, …

Ich denke nicht, dass es nötig ist jeden einzelnen Teil der cms4ds.css zu erklären. Wer dies möchte, sollte auf itaris Seite vorbei schauen (http://itari.syno-ds.de). Stattdessen werde ich nur schnell erklären, wie man das Design nach den eigenen Belieben anpassen kann.

Nehmen wir als Beispiel diese Zeile:

```
h4          {font:13 Georgia, Serif;color:#69c;}
```

Jede einzelne der Zeilen in der CSS beginnt mit der Angabe auf welchen Bereich sie zutrifft. Hier handelt es sich dabei um alle, mit h4 formatierten, Überschriften. Es folgt eine Klammer „{“ und die erste Deklaration. Zunächst geben wir an, was genau wir ändern möchten. Hier handelt es sich mit dem Begriff „font“ um Schriftgröße und Schriftart. Hinter dem Doppelpunkt folgt dann, wozu es

[83] „Server Side Includes“, erweiterte Funktionen des Webservers werden so eingeschalten, welche aus Sicherheitsgründen nicht für alle Ordner gelten dürfen.

geändert werden soll. Bei obigem Beispiel also zu einer Schrifthöhe von 13 Pixel und einer neuen Schriftart. Es wird empfohlen, mehrere Schriftarten oder am Ende eine Schrift-Familie anzugeben. In diesem Beispiel ist die Standard-Schriftart „Georgia“. Ist diese, aus welchem Grund auch immer, nicht vorhanden, wird auf den nächsten Begriff in der Reihenfolge zurückgegriffen. „Serif“ ist keine Schriftart, sondern eine Schriftartenfamilie. Ist „Georgia“ also nicht vorhanden, weicht der Browser auf eine andere Schriftart aus, welche zu dieser Gruppe gehört.

Nachdem ein Semikolon gesetzt wurde, geht es weiter. „Color“ meint natürlich die Farbe welche unsere h4-Überschrift später haben wird. Es gibt zwei Wege, Farben zu definieren, welche von jedem aktuellen Browser korrekt interpretiert werden sollten.

Die erste nutzt für die 16 Grundfarben einfache Namen wie „black“ oder „red“. Die Netscape-Entwickler wollten dies noch weiterführen und haben daher noch mehr Möglichkeiten in ihren Browser eingebaut. Diese sind, im Gegensatz zu den 16 wichtigen, nicht Teil des html-Standards und können daher falsch interpretiert werden.

Um genaue Farben anzugeben, gibt es daher noch eine andere Methode. Sogenannte „RGB-Werte“ verwandeln Farben in einen recht simplen, sechsstelligen Zahlen- und Buchstabencode. Beginnend mit einer Raute („#“) werden dabei die jeweiligen Anteile von Rot, Grün und Blau angegeben. Für jede Stelle gibt es 16 Möglichkeiten. Zunächst die Zahlen von 0 bis 9 und für 10-15 werden die Buchstaben A-F verwendet. So ergeben sich am Ende 256 Farben welche per html-Code übertragen werden können.

Soviel zu einer kleinen Einführung in CSS wie es auch von itari gebraucht wurde.

11.6 Javascript

Ganz am Anfang habe ich geschrieben, was das cms4ds so besonders macht: seine Geschwindigkeit. Und warum? Weil itari sehr sparsam mit serverseitigen Programmiersprachen wie PHP ist. Stattdessen ist das Herz des CMS4DS fast ausschließlich JavaScript.

Also stürzen wir uns nun auf die cms4ds.js. Wie die Dateiendung „.js“ schon verrät, enthält diese Datei keine einzige Zeile PHP oder html sondern ausschließlich Javascript. Sie ist wohl eine der längsten und kompliziertesten Dateien im gesamten Verbund. Doch die Funktionen dort steuern einen großen Teil des CMS.

```
var isie = /msie/i.test(navigator.userAgent) && !window.opera;
var myXMLHTTPRequest = (window.XMLHttpRequest)?
                        new XMLHttpRequest():
                        new ActiveXObject("Microsoft.XMLHTTP");
var d0,d1=0,d2=0,d3; d0=new Date().getTime();
if (!document.getElementsByClassName) {
          document.getElementsByClassName = function(className) {
                    var children = document.getElementsByTagName('*') || document.all;
                    var elements = new Array();
                    for (var i = 0; i < children.length; i++) {
                              var child = children[i];
                              var classNames = child.className.split(' ');
                              for (var j = 0; j < classNames.length; j++) {
                                        if (classNames[j] == className) {
                                                  elements.push(child);
                                                  break;
                                        }
                              }
                    }
                    return elements;
```

```
        }
}
function $(e) { return document.getElementById(e); }
function $$(e){ return document.getElementsByClassName(e); }
```

Die erste Zeile überprüft den Browser. Die nächsten legen ein paar Variablen an, die insbesondere für die Zeitmessung am unteren Ende der Seite benötigt werden. Der lange mittlere Teil beschreibt die neue Funktion document.getElementsByClassName. Diese macht es möglich bei einem Zugriff auf ein html-Objekt statt den Namen des Objekts, den Namen dessen Klasse zu verwenden.

In der letzten Zeile wird dann eine weitere Funktion hinzugefügt, die eigentlich nicht viel mehr macht, als den Namen zu kürzen. (Ja, Entwickler sind faul)

Die Zeile davor liefert statt den Klassennamen, die ID zurück, macht aber eigentlich auch nicht viel anderes als die ihm folgende Zeile, denn sie kürzt nur den Namen einer bereits vorhandenen Funktion.

```
function LoadHTML(request){
d1=new Date().getTime();
  myXMLHTTPRequest.open("GET", request, false); myXMLHTTPRequest.send(null);
  $('content').innerHTML=myXMLHTTPRequest.responseText;
d2=new Date().getTime();
}
function LoadHTML2(request){
d1=new Date().getTime();
  myXMLHTTPRequest.open("GET", request, false); myXMLHTTPRequest.send(null);
  $('index').innerHTML=myXMLHTTPRequest.responseText;
d2=new Date().getTime();
}
```

Diese beiden Funktionen werden erst später wirklich wichtig, wenn wir uns dem RSS-Feed nähern. Denn diese Funktionen machen es möglich, dass der Feed den Titel und den Inhalt abfragt.

```
var counter;
var ref=0;
function show(i){
  $$('content')[ref].style.display="none";
  $$('content')[i].style.display="block";
  histFrame.location.search=i;
}
function make_index() {
 var l=$('content').childNodes.length;
 var i=0;
 var j=0;
 var out="";
while(i<l) {
  if( $('content').childNodes[i].firstChild != null) {
    out+="<div class='index' onclick='show("+j+")'>"
       +$('content').childNodes[i].getElementsByTagName('H3')[0].innerHTML+"</div>";
    $$('content')[j].style.display='none';
    ++j;
    }
  ++i;
  }
myXMLHTTPRequest.open("GET", "cms4ds_log.php?loc="
  +location.pathname+location.search, false); myXMLHTTPRequest.send(null);
$('counter').innerHTML=
  $('counter').innerHTML.replace('#',myXMLHTTPRequest.responseText);
$('index').innerHTML=out;
$$('content')[0].style.display='block';
d3=new Date().getTime();
$('timer').innerHTML=$('timer').innerHTML.replace('#','AJAX-Request: '
```

```
  +((d2-d1)/1000)+' sek. | Page: '+((d3-d0)/1000)+' sek.');
}
```

Nachdem ein paar weitere Variablen definiert wurden, folgt die Funktion show(). Diese kümmert sich um das Beitrags-Menü rechts unten und schaltet zwischen den Beiträgen hin und her. Was dem Nutzer verborgen bleibt, ist dass die URL geändert wird um den „Zurück“-Knopf am Browser eine Chance zu geben, das Richtige zu tun.

Wie bereits beschrieben, werden die Beiträge anhand der h3-Überschriften unterteilt und mit Namen verpasst. Die Funktion make_index() erledigt genau dies. Sie läuft den gesamten Inhalt der Seite ab und richtet die Navigation für die Beiträge entsprechend ein.

Ist der Index fertig und die Seite geladen, wird die cms4ds_log.php aufgerufen und mittels PHP wird der Seitenaufruf geloggt um später jeden Aufruf minuziös verfolgen zu können. Die Zahl der Benutzer wird außerdem aktualisiert (um eins erhöht).

```
function showme(s) {
  var found=0, page='', id='';
  s=decodeURIComponent(s.substr(1)); sa=s.split('&');
  for(var i=0; i< 0) location.pathname=encodeURI('cms4ds/'+page+'.html?id='+id);
  for(var i=0; i< $$('index').length; ++i)
    if (id == $$('index')[i].innerHTML) {
      $$('content')[i].style.display="block"; ref=i; found=1;
      histFrame.location.search=i;
      }
    else
      $$('content')[i].style.display="none";
  if (found == 0) {
      $$('content')[ref].style.display="block";
      }
}
```

Die Funktion showme() ist ein Teil der Suche. Die Funktion selber ist nicht in der Lage, eigenständig die Beiträge zu durchforsten. Stattdessen nimmt es das Ergebnis entgegen und ruft dieses auf. Die eigentliche Suche übergibt die Rubrik und die ID des Artikels. **Daher funktioniert die Suche nur zuverlässig wenn alle Rubriken unterschiedliche Namen haben!** Wenn irgendetwas falsch gelaufen ist und showme() kein Ergebnis finden kann, leitet es wieder zur letzten Seite zurück.

```
function searchAll(s) {
$('content').innerHTML='';
if (s!='') {
  d0=new Date().getTime();
  LoadHTML("cms4ds.php?like="+s);
  for (var i=0; i<$('content').childNodes.length; ++i)
    if ($('content').childNodes[i].nodeType == 1)
      $('content').childNodes[i].innerHTML
        =$('content').childNodes[i].innerHTML.replace(eval('/('+s+')/gi'),'<u>$1</u>')
  }
if ($('content').innerHTML=='')
  $('content').innerHTML='<div><h3>keinen Suchbegriff gefunden</h3></div>';
make_index();
}
```

Nun zur eigentlichen Suche. SearchAll() ruft mit Hilfe von AJAX die Datenbank auf und sucht nach Übereinstimmungen. Nachdem am Anfang der „content“, also der Mittelteil der Seite, geleert wurde, wird es jetzt mit dem Ergebnis gefüllt.

```
function bookmark(s) {
  url=window.location.href+'?id='+s;
  if (isie) window.external.AddFavorite(url,s); else window.sidebar.addPanel(s,url,'');
}
```

Die Funktion bookmark() stellt sicher dass eine Seite vom Browser vernünftig als Bookmark/Favorit gespeichert werden kann. Da es hier Unterschiede zwischen den Browsern gibt, wird die Funktion entsprechend abgesichert.

```
function history(){
  if (histFrame.location.search) {
    his = histFrame.location.search.substr(1);    // remove '?'
    if (his != ref) {                             // poll return on no change
      $$('content')[ref].style.display="none";
      $$('content')[his].style.display="block";
      ref=his;
      }
    }
  window.setTimeout(history,1000);                // Timer
}
```

Damit wären wir schon fast am Ende angelangt. Das Problem der History des Browsers liegt darin, dass alle Beiträge vollständig geladen werden und er somit nicht zwischen ihnen unterscheidet. Mit einem Klick auf „Zurück“ im Browser würde man daher einen zu großen Sprung machen. Um dies zu verhindern, hat itari an eine eigene Funktion gedacht, die dem Browser die Arbeit abnimmt und zielsicher zum vorherigen Beitrag leitet. Die Funktion wird jede Sekunde aufgerufen. In der letzten Zeile steht zwar eintausend, doch Javascript arbeitet wie die meisten Programmiersprachen in Millisekunden und muss daher mit dem Wert „1000“ versorgt werden. Es prüft dann, ob im „histFrame“ unter „location.search“ eine Änderung stattgefunden hat. Trifft dies zu, wechselt sich der Beitrag.

Damit hätten wir uns durch das Herz von itaris CMS4DS gekämpft. Von nun an, ist das CMS prinzipiell zur Arbeit bereit. Doch itari hat natürlich nicht hier aufgehört. Uns steht noch eine Tour durch die zusätzlichen Funktionen wie dem RSS-Feed und der Datenbankanbindung bevor.

11.7 CMS4DS+SQL=?

Wie die Überschrift schon symbolisiert: Wir stürzen uns jetzt auf die Möglichkeit, eine SQL-Datenbank mit dem CMS4DS zu verknüpfen. Die Datenbank muss über ein geeignetes Admin-Programm zunächst erstellt werden.

Sehen wir uns einmal an, in welcher Form die Datenbank aufgebaut werden soll:

```
CREATE TABLE cms4ds_content (
  Content_ID int(11) NOT NULL auto_increment,
  TS timestamp NOT NULL default CURRENT_TIMESTAMP on update CURRENT_TIMESTAMP,
  Titel varchar(200) collate latin1_general_ci NOT NULL,
```

```
  Titel_Datum datetime default NULL,
  Hide_Date char(1) collate latin1_general_ci default NULL,
  Content varchar(32000) collate latin1_general_ci default NULL,
  Rubrik varchar(200) collate latin1_general_ci default NULL,
  Sequence int(11) default NULL,
  PRIMARY KEY  (Content_ID)
)
```

Content_ID: Existiert ausschließlich zur besseren Handhabung.

TS: Enthält das Datum der letzten Änderung, wird nicht direkt vom CMS genutzt.

Titel: Enthält eine Zeichenfolge, welche dem Namen des Beitrages entspricht.

Titel_Datum: Hier wird das Datum der Veröffentlichung vermerkt. Das Datum dient außerdem als sekundäres Suchkriterium, welches dazu genutzt wird um die Artikel zu ordnen. (Nach dem Titel)

Hide_Date: Ist hier der Wert „y“ eingefügt, wird das Datum in der Ausgabe versteckt.

Content: Enthält den eigentlichen Beitrag.

Rubrik: Gibt an, zu welcher Rubrik der Beitrag gehört. Es können auch mehrere Werte, mit Komma getrennt, angegeben werden.

Sequence: Wenn benötigt, kann hier eine manuelle Reihenfolge für die Sortierung der Beiträge in Form einer Zahl angeben. Es wird dabei aufsteigend sortiert.

Nun müssen wir noch dafür sorgen, dass ein Zugriff auf die Datenbank erfolgen kann. Dazu wird die Datei „cms4ds.php.inc“ verwendet. Die anderen Dateien enthalten einen entsprechenden Aufruf unter Verwendung des Befehls „require“.

```
<?php
$conn = @mysql_connect("localhost","root");
mysql_select_db("cms4ds",$conn);
$editor='cms4ds_editor.php?action=';
?>
```

In der zweiten Zeile werden Benutzername und Passwort angegeben. **Dieser Teil muss also in der Regel angepasst werden!**

Die dritte Zeile enthält den Namen der Datenbank und die vierte Zeile den Link zum Editor, welcher auch angepasst werden kann, wenn benötigt.

Doch nun zur eigentlichen Abfrage, welche in cms4ds.php eingefügt wird:

```
<?php
function iso8859_mydecode($html){   // simple translation of german letters
  $a = array('ä'=>"xC3xA4",'ö'=>"xC3xB6",'ü'=>"xC3xBC",
             'Ä'=>"xC3x84",'Ö'=>"xC3x96",'Ü'=>"xC3x9C",'ß'=>"xC3x9F");
  return strtr($html,$a);
}
function utf8_mydecode($html){      // reverse simple translation of german letters
  $a = array("xC3xA4"=>'ä',"xC3xB6"=>'ö',"xC3xBC"=>'ü',
             "xC3x84"=>'Ä',"xC3x96"=>'Ö',"xC3x9C"=>'Ü',"xC3x9F"=>'ß');
  return strtr($html,$a);
```

```
}
$t0=sscanf(microtime(),"%f %s");
require "cms4ds.php.inc";
$where=
  preg_replace('/([^a-zA-Z%'0-9äöüÄÖÜß_(), ])/','',utf8_mydecode($_REQUEST['where']));
$recs = mysql_query("select * from cms4ds_content where find_in_set('"
  .$where."',replace(Rubrik,' ',',')) order by Sequence, Titel_Datum desc");
$out='';
while ($rec = mysql_fetch_assoc($recs)) {
$out.='<div class="content" style="display:block"><h3 onclick="bookmark(''
.$rec['Titel'].'')">'.$rec['Titel'].'</h3>'
.($rec['Hide_Date']=='y'?'':'<i>'.substr($rec['Titel_Datum'],0,10))
.($rec['Autor']==''?'':' - ').$rec['Autor'].'</i><p>'.$rec['Content'].'</p>';
if (substr($_SERVER['REMOTE_ADDR'],0,7)=='192.168') {
  $out.='<p style="position:absolute;top:150px;margin-left:-50px">'
  .'<a target="_blank" onclick="window.open(''.$editor
  .'new','','top=200,left=300,width=600,height=700')">new/lt;/a><br/>'
  .'<a target="_blank" onclick="window.open(''.$editor
  .'search&Content_ID='.$rec['Content_ID']
  .'','','top=120,left=250,width=616,height=540')"%gt;edit</a></p>';
  }
$out.='</div>';
}
@mysql_close($conn);
$t1=sscanf(microtime(),"%f %s");
print $out;
?>
<!--#set var="t" value="<?php print 'PHP: '.($t1[0]-$t0[0]).' sek. | ' ?>" -->
```

Einmal Schritt für Schritt:

Zunächst werden die „deutschen Sonderzeichen“ (ä,ö,ü,Ä,Ö,Ü) in Code umgewandelt, damit es nicht zu Problemen kommt.

Dann wird eine Variable mit Zeitstempel erstellt und am Ende mit einer zweiten abgeglichen um die Zeit des Zugriffs messen zu können.

Nun folgt eine weitere Zeichenüberprüfung. Doch dieses Mal werden Probleme nicht in Codes umgewandelt, sondern rigoros gelöscht. Also: Vorsicht mit Sonderzeichen.

Und endlich folgt dann der Datenbankzugriff.

Bei einer Abfrage wird die Sortierung zuerst anhand des „sequenc“-Wertes versucht. Sollten alle diese Werte gleich sein, wird auf das Datum zugegriffen.

Am Ende sieht dann die Struktur eines einzelnen Beitrages aus wie folgt:

```
<div class="content" style="display:block" >
// damit auch ein Bookmark-Integration erfolgen kann, wird der Titel hierfür vorbereitet
<h3 onclick="bookmark('Titel')">Titel</h3>
//falls das Hide_Date ungleich y ist, dann wird zudem das Titel_Datum ausgeben
//falls der Autor existiert wird er auch mit ausgegeben, getrennt mit einem '-'
<i>Titel_datum - Autor</i>
<p>Content</p>
//falls die Ausgabe im lokalen Netz erfolgt (Adress-Raum 192.168.x.x),
//dann wird der Editor-Aufruf eingebaut
<p style="position:absolute;top:150px;margin-left:-50px">'
  .'<a target="_blank" onclick="window.open(''.$editor.'new','','top=200,
    left=300,width=600,height=700')">new</a><br/>'
  .'<a target="_blank" onclick="window.open(''.$editor.'search&Content_ID='
  .$rec['Content_ID'].'','','top=120,left=250,width=616,height=540')">edit</a></p>
</div>
```

Ich denke die Kommentare erklären alles von selbst.

Itari hat auch an eine Datenbank zum Erfassen aller Besucher gedacht. Diesen Teil möchte ich mir hier aber sparen, da er nicht elementar für die Funktionsweise des CMS ist. Nur noch einmal der kurze Hinweis: Wer diese Funktion in vollem Umfang nutzen möchte, muss vorher die entsprechende Datenbank erstellen.

11.8RSS

Jede moderne Website stellt einen bereit. RSS-Feeds. Sie werden verwendet um sich regelmäßig ändernde Seiten, welche Beiträge nach Zeit geordnet enthalten, mit externen Programmen ansehen zu können und diese zu abonnieren. Wie wir bereits gesehen haben, ist itaris CMS moderner als so manch aufgeblasenes fertig-CMS. Daher darf natürlich auch ein RSS-Feed nicht fehlen.

Den entsprechenden Link in der header.html haben wir ja bereits gesehen. Dieser führt uns zur Datei cms4ds_rss.php.

```
<?php
function iso8859_mydecode($html){         // simple translation of german letters
  $a = array('ä'=>"xC3xA4",'ö'=>"xC3xB6",'ü'=>"xC3xBC",
             'Ä'=>"xC3x84",'Ö'=>"xC3x96",'Ü'=>"xC3x9C",'ß'=>"xC3x9F");
  return strtr($html,$a);
}
header('Content-Type: application/xml');
print '<?xml version="1.0" encoding="UTF-8"?>'; ?>
<?php
print '<rss version="0.91"><channel><title>cms4ds-News-Feed</title>'
      .'<link>http://'.$_SERVER['HTTP_HOST'].$_SERVER['PHP_SELF'].'</link>'
      .'<description></description><language>de</language>';
require "cms4ds.php.inc";
$recs = mysql_query("select Titel,Rubrik,Titel_Datum from cms4ds_content
                              order by Titel_Datum desc limit 2");
while ($rec = mysql_fetch_assoc($recs))
      print '<item><title>'.iso8859_mydecode($rec['Titel']).'</title><link>'
            .'http://'.$_SERVER['HTTP_HOST'].dirname($_SERVER['PHP_SELF']).'/'
            .$rec['Rubrik'].'.html?id='
            .rawurlencode(iso8859_mydecode($rec['Titel'])).'</link></item>';
print '</channel></rss>';
?>
```

Dieser php-Aufruf gibt eine XML-Datei nach RSS-Standard 0.91 wieder. Der Aufruf ähnelt dem eines normalen Such-Aufrufs bei dem alle Beiträge nach Datum geordnet werden. Im Quelltext sind zwei Teile rot hervorgehoben. Diese sollte man an die eigenen Bedürfnisse anpassen. Der erste stellt dabei den Namen des Feeds und die zweite die Anzahl der darzustellenden Beiträge dar.

```
<?xml version="1.0" encoding="UTF-8"?>
<rss  version "0.91">
 <channel>
  <title>cms4ds-News-Feed</title>
  <link>http://syno/cms4ds/cms4ds_rss.php</link>
  <description></description>
  <language>de</language>
  <item>
   <title>cms4ds als RSS-Feed</title>
   <link>http://syno/cms4ds/rss.html?id=cms4ds%20als%20RSS-Feed</link>
  </item>
  ...
 </channel>
```

```
</rss>
```

Der obige Text stellt dar, wie eine fertige XML-Seite aussehen könnte.

Wer RSS-Feeds von anderen Seiten einbinden möchte, kann auf bereits vorhandene Funktionen zurückgreifen, welche itari uns mitliefert. Mehr Informationen dazu, gibt es auf seiner Seite.

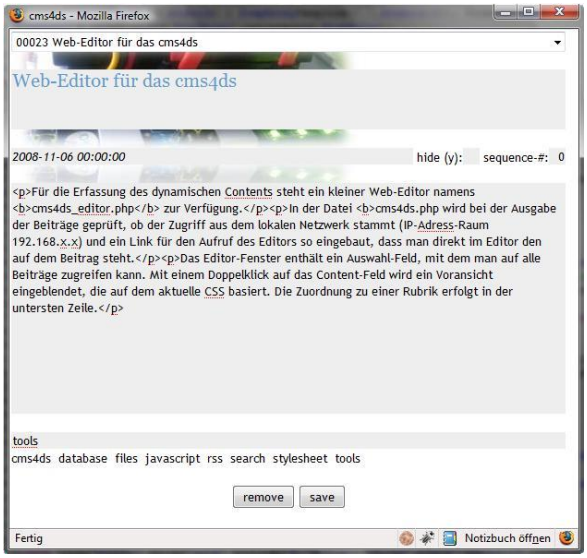
Zur Suche auf der eigenen Seite unter Verwendung des OpenSearchDescription-Protokolls gibt es auch eine eigene XML-Datei. Diese wird unter anderem von Browsern genutzt, um die Suchanfragen aus den kleinen Fenstern rechts oben im Browser durchzuführen. Auch auf diese möchte ich hier allerdings nicht näher eingehen.

11.9 Tools

Wer sich bisher aufmerksam durch die Quelltexte gearbeitet hat, dem werden ein paar merkwürdige Zeilen aufgefallen sein, auf die ich nicht genau eingegangen bin.

```
//falls die Ausgabe im lokalen Netz erfolgt (Adress-Raum 192.168.x.x),
//dann wird der Editor-Aufruf eingebaut
<p style="position:absolute;top:150px;margin-left:-50px">'
  .'<a target="_blank" onclick="window.open(''.$editor.'new','','top=200,
    left=300,width=600,height=700')">new</a><br/>'
  .'<a target="_blank" onclick="window.open(''.$editor.'search&Content_ID='
  .$rec['Content_ID'].'','','top=120,left=250,width=616,height=540')">edit</a></p>
</div>
```

Die Datei cms4ds_editor.php enthält einen Texteditor, mithilfe dessen sich die einzelnen Seiten unkompliziert bearbeiten lassen. Wenn eine Überprüfung der IP ergibt, dass die Anfrage von einem Computer kommt, dessen Adresse mit 192.168 beginnt, wird als weiteres Fenster der Editor geöffnet. Alle Adressen innerhalb Ihres Netzwerks beginnen so, sollten Sie nicht stark an ihren Netzwerkeinstellungen gedreht haben.



Wie bereits beschrieben, wird eine zweite Datenbank angelegt, wo alle Zugriffe gespeichert werden. Um aber nicht diese Datenbank kompliziert auslesen zu müssen, gibt es auch hierfür das passende PHP-Skript. Der Aufruf erfolgt über cms4ds_showlog.php

11.10 Ein Ausblick

Doch weil itari ist wie er ist, arbeitet er natürlich immer weiter. So findet man nun sowohl auf seiner Seite, als auch im Forum, weiterführende Themen, welche allerdings weit über das Konzept eines kompakten CMS hinausgehen und daher hier nicht erklärt werden sollten. Dennoch möchte ich wenigstens darauf hinweisen. Es handelt sich dabei unter anderem um Themen wie die Einbindung von Drittanwendungen wie Cooliris. Aber auch die Möglichkeit des Verfassens von Kommentaren lies itari nicht ungenutzt.

12 .htaccess Zugriffsschutz

Über einfache Zugriffsbeschränkungen wurde ja bereits gesprochen. Doch „htaccess“ können noch deutlich mehr als nur einfache Passwortabfragen. Da mir Sicherheit ja sehr am Herzen liegt, wie Sie sicherlich bereits bemerkt haben, bekommt dieses Thema ein eigenes Kapitel.

Der Begriff „htaccess“ kommt von „hyper-text-access“. Also Zugriffsbeschränkung auf Internet-Text. Es handelt sich dabei um einen Standard, welcher von vielen Servern unterstützt wird, unter anderem dem Apachen. Somit ist dies keine Modifikation, welche Probleme bezüglich der Garantie machen kann, sondern eine standardmäßige Funktion des verwendeten Webservers.

Zunächst zum Thema Weiterleitung. Offiziell gibt es ja auch mit html eine Möglichkeit der Weiterleitung. Diese ist allerdings unter Programmierern verpönt, da sie weder nutzerfreundlich noch sicher ist. Eine Weiterleitung welche direkt vom Webserver gesteuert wird, sollte vom Nutzer nicht bemerkt werden und ist auch sicherheitstechnisch zu befürworten. Somit sollten Sie immer auf htaccess setzen statt meta-Tags in html, wenn Sie eine Wahl haben.

12.1 Die Datei

Eine htaccess-Datei kann mit einem einfachen Texteditor erstellt werden. Windows-Nutzer können dabei vom integrierten Editor Gebrauch machen. Wer gerne erweiterte Funktionen genießen möchte, sollte sich Alternativen wie „Notepad++“[84] anschauen, welcher als Open-Source verfügbar ist. Eine solche Datei ist für einen Ordner und wahlweise auch deren Unterordner gültig. Also kann es immer nur eine einzige pro Ordner geben, weshalb sich auch keiner Gedanken um Dateinamen gemacht hat. Daher bekommen hyper-text-access-files einfach den Dateinamen „.htaccess“. Vergessen Sie den Punkt nicht, denn er versteckt die Datei vor einigen Prozessen und erhöht so die Sicherheit! Auch wird die Datei nur so über das Web nicht abrufbar (was wieder eine Sicherheitslücke darstellen würde).

12.2 Weiterleitungen

Nun erstellen Sie eine neue Datei „.htaccess“. Anders als html oder PHP müssen nicht andere Strukturen erstellt oder Formate definiert werden. Daher schreiben Sie einfach in Zeile eins:

```
Redirect / http://www.zielurl.de
```

Nach dem hochladen auf Ihre DS öffnen Sie den Browser. Wenn Sie nun den Ordner ansteuern, in dem die entsprechende .htacces liegt, werden Sie automatisch auf „http://www.zielurl.de“ weitergeleitet.

Nun zu einem anderen Szenario:

Sie geben ihrem Freund den Link „www.ihre-domain.de/tagebuch“ und wollen ihn damit auf den Photo Station Blog umleiten. Doch zurück zu Hause erinnern Sie sich, dass der Link zum Blog „/blog“ ist und nicht, wie Sie ihm gesagt hatten „/tagebuch“. Also was machen? Legen Sie doch einfach eine „.htaccess“ in den Stammordner Ihres Webservers „/web“ und fügen Sie ihr folgende Zeile hinzu:

[84] http://notepad-plus-plus.org/

```
Redirect /tagebuch/ http://www.ihre-domain.de/blog
```

Daraus ergibt sich dann:

Redirect /[*Verzeichnis*] [*Zieladresse*]

Wobei „Verzeichnis“ optional ist, aber nicht der Schrägstrich!

12.3 IP-Sperre

Als nächstes sollen einzelne Teilnehmer des Internets gezielt von Ihrem Server ausgesperrt werden. Die Rede ist von einer IP-Sperre. Sie können übrigens verschiedene Methoden welche hier besprochen werden kombinieren. So können Sie beispielsweise zuerst IPs filtern und dann alle, die den Test bestanden haben, auf eine andere Adresse weiterleiten.

Aber nun zurück zu unserem Anliegen:

```
# Zugriff verbieten außer für Nutzer des internen Netzes und Kunden der dt. Telekom
order deny, allow
deny from all
allow from 192.168
allow from .t-home.de
```

Obwohl die erste Zeile noch nichts direkt mit unserem Vorhaben zu tun hat, stellt sie die erste Neuerung dar. Es handelt sich dabei um einen Kommentar, welcher vom Webserver vollständig ignoriert wird. Derartiges findet sich in jeder Maschinensprache. In htaccess beginnen jene mit „#“.

Wie bereits im Kommentar beschrieben, blockiert das Beispiel-Skript zunächst alle Zugriffe. Dabei gibt die erste nicht-kommentierte Zeile zunächst an, in welcher Reihenfolge die Angaben notiert wurden. Es gibt eine einfache Regel: Beginnen Sie mit dem, was Sie NICHT möchten. In den meisten Fällen also „deny“.

In der ersten und einzigen „deny“-Zeile steht somit „deny from all“, welches alle Zugriffe blockiert. Ohne die nachfolgenden Zeilen, würden Sie sich also von Ihrem eigenen Server aussperren.

Als nächstes werden im Beispiel alle Zugriffe erlaubt, welche von einem Computer erfolgen, der in das Netz „192.168.x.x“ eingebunden ist. In den meisten Fällen sollte das Ihr Heimnetz sein. Also folgt in der nächsten Zeile ein „allow from“ (erlaube von), gefolgt vom IP-Bereich. Die letzte Zeile funktioniert nach demselben Muster, nur mit dem Unterschied, dass statt einer IP, eine Domain zum Einsatz kommt.

Anhand der Erklärungen ergibt sich folgender Syntax:

[allow | deny] from [all | *IP* | *host*]

> ***In diesem Muster werde ich auch die anderen Regeln zusammenfassen. Von den Elementen in den Klammern muss man jeweils eines auswählen und erhält dann eine gültige Formulierung. Kursiv geschriebene Elemente können jedoch nicht 1:1 übernommen werden. „IP“ steht beispielsweise für eine gültige IP-***

Adresse und „host“ für eine Domain. Ein paar Beispiele, welche sich aus der obigen Regel ergeben könnten:

allow from 127.0.0.1

deny from aol.com

Doch perfekt ist auch diese Methode nicht. Die einzige Möglichkeit für einen Server, die IP des Senders zu bestimmen, besteht darin bestimmte Teile des Datenpakets auszulesen, welche eben diese Information bereithalten. Nun ist es aber möglich dies zu manipulieren und der Server erlaubt den Zugriff möglicherweise zu unrecht. Daher sollte diese Form des Zugriffsschutzes immer nur in Kombination mit einer anderen, wie einer Passwortabfrage, genutzt werden.

12.4 Eigene Fehlerseiten

Wie bereits beschrieben, gibt es eine einfache Möglichkeit benutzerdefinierte Fehlerseiten anzuzeigen. Allerdings gilt dies nur für „Error 404-Not Found“, also dass die angeforderte Datei konnte nicht gefunden werden. Dafür reicht eine Datei namens „missing.html“ im „/web“-Verzeichnis. Mittels htaccess können Sie aber auch viele weiteren Fehler definieren. Eine vollständige Liste aller Status-Nummern finden Sie auf SelfHTML[85]. Die wichtigsten Fehler, welche auch auf einer DS immer mal auftreten können, habe ich hier zusammengefasst:

Status-Nummer	Offizielle Nachricht	Übersetzung und Beschreibung
401	Unauthorized	Nicht autorisiert – Der Client konnte sich nicht, wie vom Server gefordert, mit Nutzerdaten identifizieren
403	Forbidden	Verboten – Der Server möchte die angeforderten Dateien nicht senden. Ein Grund dafür kann z.b. eine htaccess-Datei sein, in der dessen IP vom Filter aussortiert wird.
404	Not Found	Nicht gefunden – Die angeforderte Datei konnte nicht gefunden werden. Bei eben jener Fehlermeldung würde die DS normalerweise versuchen die Datei „missing.html“ zu öffnen. Existiert diese nicht, wird ihnen die Synology-Fehlermeldung präsentiert.[86]
408	Request Timeout	Zeitspanne abgelaufen – Jeder Verbindung wird eine gewisse Zeit eingeräumt, bis ein Ergebnis präsentiert werden muss. Ist diese Überschritten, obwohl ihr Server gefunden wurde, tritt dieser Fehler auf.

[85] http://de.selfhtml.org/servercgi/server/httpstatuscodes.htm#uebersicht

[86] Gemeint ist folgende Fehlermeldung:

500	Internal Server Error	Interner Server-Fehler – Sollte ein Problem im Server oder im auszuführenden Skript aufgetreten sein, wird dieser Fehler zurückgegeben. Häufige Ursache ist ein Fehler in der Programmierung der Seite.
503	Service Unavailable	Dienst nicht erreichbar – In diesem Fall wird der Server zwar erreicht, liefert aber keine Daten zurück, da er überlastet ist.

Doch nun endlich zurück zum Thema. Der folgende Inhalt muss in der htaccess-Datei liegen, welche sich im Stammordner des Webservers, also „/web“, befindet:

```
# Die Fehler 401, 403 und 404 werden auf error.php weitergeleitet
ErrorDocument 401 /error.php
ErrorDocument 403 /error.php
ErrorDocument 404 /error.php
```

Die entsprechende Datei „error.php“ kann auch in einem anderen Ordner liegen. Der Pfad muss dabei mit angegeben werden (z.B. „*ErrorDocument 401 /errors/html-401.php*“). Die Datei sollte dann Informationen für den Nutzer enthalten, in denen er über den aufgetretenen Fehler informiert wird und eventuell auch, wie er Sie als Betreiber davon in Kenntnis setzen kann (Formular, E-Mail-Adresse, …).

Wenn Sie keine eigenen Fehlermeldungen aufsetzen, bekommt man kurze, knappe, häufig auf Englisch verfasste Meldungen vom Apache.

Abschließend noch der Syntax:

ErrorDocument [*Error-Code*] /[*Pfad zur Hilfedatei*]

12.5 Passwortschutz

Doch nun zur eigentlichen Stärke von htaccess. Dem Passwortschutz:

```
# Grundlegender Passwortschutz
AuthType Basic
AuthName “Passwortschutz-Beispiel“
AuthUserFile /passw/.htusers
Require valid-user
```

Zeile für Zeile:

AuthType Basic – Damit geben Sie den Startschuss für einen Passwortschutz. Außerdem bedeutet „Basic“, dass die Kommunikation unverschlüsselt erfolgen wird. Alternativ können Sie dort „Digest“ einsetzen. Allerdings wird diese verschlüsselte Variante nicht von allen Browsern unterstützt. Entscheiden Sie also selber.

AuthName – Diese Wortgruppe spielt keine wichtige Rolle und existiert nur, damit Sie bei verschiedenen Systemen nicht die Übersicht verlieren.

AuthUserFile – Nun wird es spannend. In dieser Zeile müssen sie den Link zu einer Datei angeben, welche in einem Unterverzeichnis liegt und deren Dateiname mit „.ht“ beginnt. Üblicherweise wird „.htusers“ oder „.htpasswd“ verwendet. Vorteil wenn sie einen dieser Namen verwenden: Richtig konfigurierte Webserver verstecken diese Datei, sodass ein Zugriff nur mittels FTP o.ä. möglich ist. Über den Inhalt dieser Datei werde ich später sprechen.

Require valid-user – Mittels dieser Zeile hauchen Sie ihrer Beschränkung leben ein. Denn nun erhält nur noch der Zugriff, der einen gültigen Benutzernamen vorweisen kann (valid-user).

Doch wie genau wird jetzt eigentlich Benutzer und Passwort definiert? Dafür erstellen wir eine neue Datei. Den Dateinamen entnehmen Sie der Angabe, welche Sie bei „AuthUserFile“ gemacht haben. In meinem Fall also „.htuser“. Genauso finden Sie dort auch den Pfad in dem Sie später die Datei speichern müssen.

```
Herbert:hd0djg4D4o6f6
Manfred:Db/H2kWNBnr5.
Werner:BsIMhXgYNGCUg
```

Ohne umständliche Definitionen enthält diese Datei wie bei htaccess üblich alle Informationen kurz und bündig. Sie können beliebig viele Benutzer definieren. Hinter jedem Benutzer setzen Sie einen Doppelpunkt und ohne Leerzeichen direkt dahinter das verschlüsselte Passwort. Die Verschlüsselung muss generiert werden. Dazu gibt es verschiedene Seiten im Internet, welche dies anbieten. Einen guten finden Sie bei SelfHTML[87]. Außerdem enthält diese Seite viele nützliche Informationen zu unserem Thema.

Syntax:

[*Benutzername*]:[*verschlüsseltes Passwort*]

Und schon haben Sie ihre Dateien geschützt.

12.6 Erweiterte Möglichkeiten des Passwort-Schutz

Doch auch hier hört htaccess noch lange nicht auf. Den ersten Punkt haben wir ja mit der „AuthType“-Alternative „Digest“ bereits gesehen.

Gehen wir noch einmal zurück zur eigentlichen „.htaccess“-Datei, welche später im Ordner liegen wird. Hinter „AuthUserFile“ können Sie eine Zeile „AuthGroupFile“ einfügen. Dahinter hängen Sie, genau wie bei „AuthUserFile“, eine Pfadangabe zu einer Datei, welche „.htgroups“ heißt.

Ein Beispiel dieser Datei:

```
Vertrauenswuerdig: Herbert Manfred
Autoren: Manfred Werner
```

[87] http://de.selfhtml.org/servercgi/server/htaccess.htm#verzeichnisschutz

Soeben haben wir zwei Gruppen erstellt. Der Gruppenname steht dabei vorne, gefolgt von einem Doppelpunkt und allen Benutzern, welche zur Gruppe gehören sollen, getrennt lediglich von einem Leerzeichen.

Doch was nutzt uns eine Einteilung in Gruppen? Damit wären wir bei den nächsten Erweiterungen. „Require valid-user“ reizt die Möglichkeiten der „Require“-Anweisung nicht einmal ansatzweise aus.

So wie von uns verwendet, wird nur ein gültiger Benutzer verlangt. Um dies einzuschränken gibt es zwei Möglichkeiten. Entweder simpel über „Require user“ gefolgt von den erwarteten Nutzernamen oder über „Require group“. Und genau da zahlen sich unsere Mühen um eine .htgroups aus:

Wenn Sie die Zeile „Require valid-user“ gegen „Require group Autoren“ ersetzen, erhalten nur noch Manfred und Werner, nicht aber Herbert Zugriff. Sobald Sie viele Nutzer zu verwalten haben, kommt ihnen eine derartig aufgespaltene Nutzerverwaltung schnell gelegen und kann viel Zeit sparen.

Syntax:

Require [valid-user | *group* | *user*] [*ausgewählte Nutzer* | *ausgewählte Gruppen*]

Kommen wir nun zur letzten erweiterten Möglichkeit:

```
[…]
<Files *.html>
Require group Vertrauenswuerdig
</Files>
```

Wenn sie die obigen Zeilen an unser bereits verwendetes Beispiel anhängen, werden die Berechtigungen für html-Dateien überschrieben. Diesmal dürfen nur Nutzer, welche der Gruppe „Vertrauenswuerdig“ angehören, auf html-Dateien zugreifen.

Syntax:

<Files *.[*Dateiendung*]>
[*Require-Anweisungen*]
</Files>

Und damit wären wir mit unserer kleinen Exkursion fast zu Ende. Nur noch ein paar abschließende Bemerkungen:

12.7 Sicherheitsprobleme trotz htaccess

Nun stellt sich am Ende noch die Frage: Wie sicher ist htaccess eigentlich? Das Thema Verschlüsselung haben wir ja bereits behandelt. Doch auch wenn unsere Passwörter verschlüsselt sind und auch so übertragen werden, ist Vorsicht geboten. So lange wie der Passwortschutz in Dateien vorliegt, gibt es auch Möglichkeiten Sie zu löschen oder gar zu manipulieren. Auch wenn der Apache sein bestes tut die .ht-Dateien zu verstecken. Solange wie es FileStation und FTP gibt, sollten Sie mit den Berechtigungen für die entsprechenden Ordner vorsichtig sein. Auch sichere Passwörter sind stets ein Thema, da Brute-Force Attacken schwer abzuwehren sind.

Noch eine letzte Bemerkung: Sie werden bei htaccess auf eine Funktion namens „Fancy Indexing“ treffen. Doch leider ist seitens Synology dessen Nutzung nicht vorgesehen. Bei Google finden sie dennoch Modifikationen welche ihnen helfen können.

12.8.htaccess-Referenz

Diese Seite soll eine Referenz zum Ausdrucken und neben die Tastatur legen sein.

Weiterleitung

Syntax	Beispiele	Erklärung
Redirect /[*Verzeichnis*] [*Zieladresse*]	Redirect /html/ http://selfhtml.de	Direkte Weiterleitung bei Angabe eines Unterordners auf Zieladresse

Client-/IP-Sperren

Syntax	Beispiele	Erklärung
order [deny | allow], [deny | allow]	order allow, deny order deny, allow	Als Einleitung zu Sperren gibt diese Zeile an, in welcher Reihenfolge die Sperren eingesetzt werden.
[allow | deny] from [all | *IP* | *host*]	Allow from all Deny from 192.168 Allow from 127.0.0.1 Deny from .google.com	Dieser Befehl ist das Herz der IP-Sperre. Gefolgt von der „order“-Anforderung können hier unbegrenzt viele Regeln aneinander gereiht werden.

Status-Code-Redirect

Syntax	Beispiele	Erklärung
ErrorDocument [*Code*] /[*Datei-Link*]	ErrorDocument 401 /missing.html ErrorDocument 403 /err/403.html ErrorDocument 503 /last.html	Sollte ein Fehler welcher als http-Status-Code definiert ist, auftreten, wird entsprechend weitergeleitet.

Passwortschutz

Syntax	Beispiele	Erklärung
AuthType [Basic | Digest]	AuthType Basic	Verschlüsselung an-/ausschalten
AuthName [*Bezeichnung*]	AuthName stammordner	Name zur Übersicht
AuthUserFile [*Datei-Link*]	AuthUserFile /access/.htusers	Link zur Datei welche „Nutzer:Passwort“ enthält
AuthGroupFile [*Datei-Link*]	AuthGroupFile /acces/.htgroups	Link zur Datei welche „Gruppe: Teilnehmer“ enthält
[*Benutzername*]:[*Passwort*]	Werner:BsIMhXgYNGCUg	Inhalt der „.htusers“-Datei
Require [valid-user | *user* | *group*]	Require valid-user Require user Werner	Abschließende Angabe, wer zugreifen darf.
<Files *.[Dateierweiterung]> [Require-Anweisungen] </Files>	<Files *.html> Require valid-user </Files>	Spezielle Beschränkungen für einzelne Dateierweiterungen.

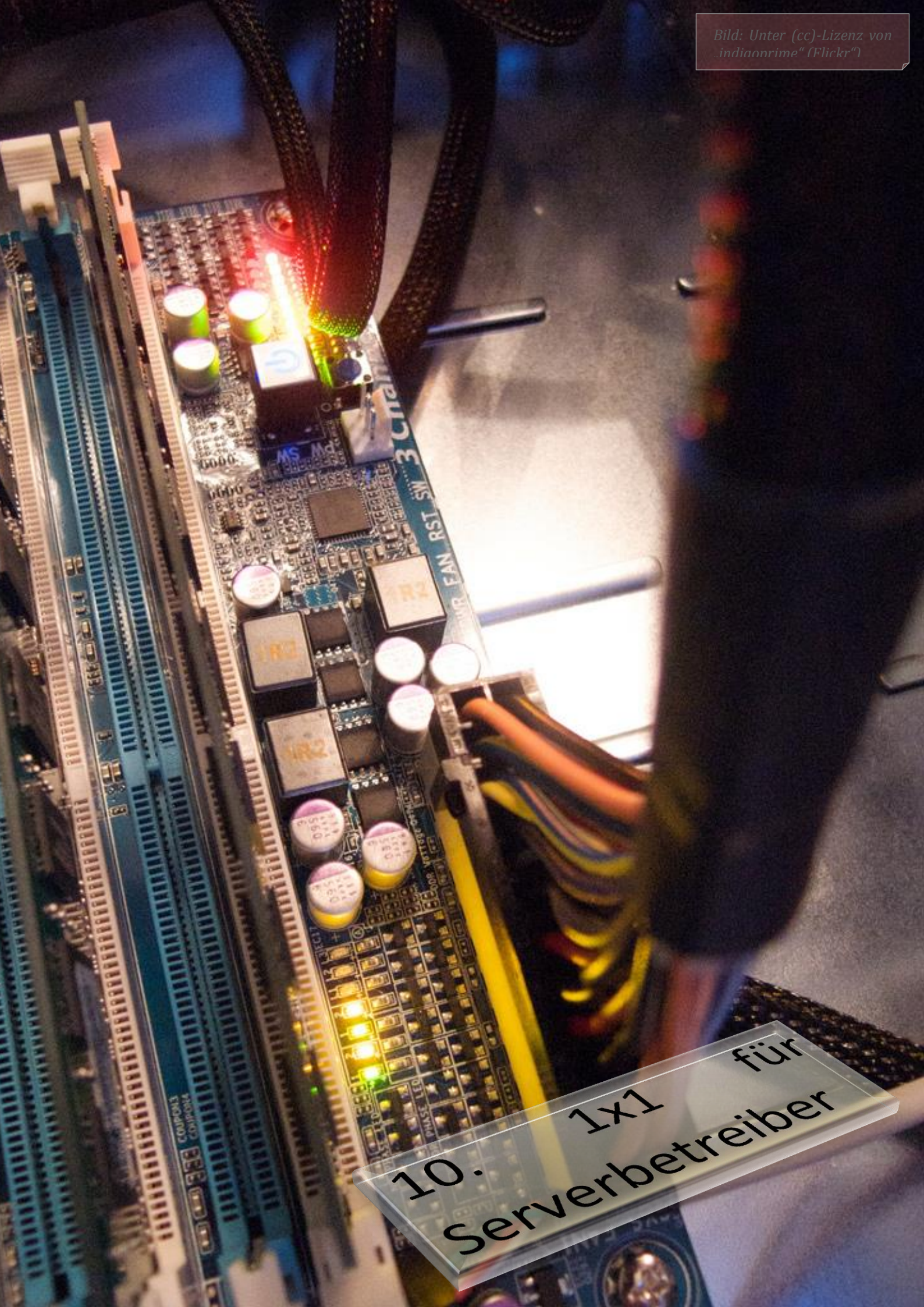


Bild: Unter (cc)-Lizenz von indiagoprime“ (Flickr“)
10. 1x1 für Serverbetreiber

13 1x1 für Server- und Webseitenbetreiber

Bevor der eigene Server womöglich noch inklusive Webseite auf das weite WWW losgelassen wird, sollte man sich ein paar wichtige Dinge vor Augen halten.

13.1 Domains, Namen & Ansprüche

Die ersten Probleme beginnen bereits beim Domain-Namen. Viele Domaininhaber mussten bereits ihre Domains wegen Namensproblemen an den Eigentümer einer Marke abtreten. Auch wenn die Domain auf den ersten Blick nur „normale“ Wörter enthält, ist Vorsicht geboten. Beinahe jedes Wort mit einem ausreichenden Wiedererkennungswert lässt sich als Marke registrieren. Nachschlagen kann man Markennamen beispielsweise beim deutschen Patent- und Markenamt (DPMA) unter http://dpma.de/. Ist eine Suche dort ohne Resultat, kann man sich in der Regel recht sicher fühlen. Wer aber hingegen dem Irrglauben unterfällt, das Markenrecht zu umgehen indem man eine klare Differenz zur Marke gibt, sollte vorsichtig sein. Hier ist das Ermessensmaß der Richter sehr weitläufig. So erging es beispielsweise dem Besitzer von „eltern-online.de“. Nach Ansicht der Richter stellte das Anhängsel „online“ keine ausreichende Differenzierung zu dem des Magazins Eltern angemeldeten Markennamen dar. Wer seine Seite ausschließlich privat nutzt hat das Glück mit dem Markenrecht nur eingeschränkt zu unterliegen, doch wie schnell man kommerziell handelt, werden wir später sehen.

13.2 Domain-Anbieter wählen

Jede Verwaltungsstelle für TLDs (Top-Level-Domains, also Domains wie .de, .com, .org, usw.) ist für die Vergabe von Domains vollständig verantwortlich. In Deutschland, für .de-Domains, ist das die DENIC (Deutsche Network Information Center). Diese Organisation hat eine gewisse Anzahl von Mitgliedern, größtenteils Unternehmen, die dann entsprechende Domains beantragen, verwalten und vergeben können. Prinzipiell ist es empfehlenswert Domains immer von Mitgliedern der jeweiligen Vergabestelle zu beziehen. Denn Drittanbieter müssen ihrerseits wiederum auf jene Zurückgreifen, was manchmal zu längeren Bearbeitungszeiten und rechtlichen Auseinandersetzungen führen kann. Mehr Informationen unter http://www.denic.de/. Dort findet sich auch eine Recherche-Möglichkeit für freie und vergebene Domains. Denn als Domain-Inhaber werden Sie mit Namen, E-Mail und Anschrift vermerkt um im Streitfall schnell Kontakt aufnehmen zu können. Die Richtigkeit dieser Daten ist in Deutschland verpflichtend und wird im Fall des Verstoßes rechtlich geahndet.

Es ist sehr wichtig dass Sie ihrem Anbieter vertrauen können. Denn er muss beispielsweise (bei bestimmten TLDs) die Aktivität der Domain bestätigen. Tut er dies nicht, etwa weil er sich mit ihnen um Zahlungen streitet oder seine Technik versagt, können sogenannte Domain-Grabber die Domain währenddessen auf den eigenen Namen registrieren. Zurück geben diese eine Domain meist nur gegen viel Geld.

13.3 Das müssen/können Sie auf ihrem Server tun

Ist der Server erst einmal erreichbar, muss auf bestimmte Dinge geachtet werden. So treffen auf Betreiber sowohl Gesetze zu, welche schon seit dem Urbeginn des Rechtssystems gelten, genauso wie die noch recht jungen Gesetze für sogenannte „Neue Medien“. Da gäbe es zum Beispiel die Gesetze zum Thema Volksverhetzung, Verleumdung, Pornografie und Copyright. Kurz gesagt: Sie haften für das, was Sie anbieten. Dabei übernehmen Sie auch eine eingeschränkte Haftung wenn ein

anderer Nutzer Daten auf ihrem NAS speichert. Die Haftung erstreckt sich dabei auf Straf- und Zivilrecht gleichermaßen. Inwiefern Sie den Nutzer von ihrem Server ausschließen können, hängt von der Vereinbarung ab, welche sie vorher getroffen haben müssen. Mehr Informationen dazu findet man im Internet unter „(Mit-) Störerhaftung“. Doch hier würde das Thema zu weit führen.

13.4 Kommerzielle Nutzung, Werbung und Impressumspflicht

Wenn ich frage, ob Sie Ihre Seite kommerziell nutzen, so werden Sie wahrscheinlich mit Nein antworten. Wenn ich Sie nun aber Frage, ob Sie Werbung auf ihrer DiskStation oder generell im Internet betreiben, ist die Wahrscheinlichkeit für ein Ja sehr viel höher. Besonders einfach macht dies beispielsweise auch der „Google AdWords“-Block der Photo Station. Das Problem dabei: Kommerziell heißt, sobald Sie Geld mit ihrer Webseite verdienen können. Das trifft auch auf Werbung zu. Und sei es nur ein kleiner Banner oder Hinweis. Auch ist zu beachten, dass Werbung auf den Internetseiten als solche gekennzeichnet werden muss.

Mit einem Kommerziellen Angebot kommt auch die Pflicht zu einem Impressum. Das Teledienstgesetz sieht dazu folgendes vor:

§ 6 (Stand 14. September 2001)
Allgemeine Informationspflichten

Diensteanbieter haben für geschäftsmäßige Teledienste mindestens folgende Informationen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar zu halten:

1. *den Namen und die Anschrift, unter der sie niedergelassen sind, bei juristischen Personen zusätzlich den Vertretungsberechtigten,*

Dies ist für Sie in jedem Fall Pflicht.

2. Angaben, die eine schnelle elektronische Kontaktaufnahme und unmittelbare Kommunikation mit ihnen ermöglichen, einschließlich der Adresse der elektronischen Post,

Kurzum: Ihre E-Mail-Adresse, welche Sie häufig kontrollieren.

3. soweit der Teledienst im Rahmen einer Tätigkeit angeboten oder erbracht wird, die der behördlichen Zulassung bedarf, Angaben zur zuständigen Aufsichtsbehörde,

Das sollte nur in Ausnahmefällen zutreffen.

4. das Handelsregister, Vereinsregister, Partnerschaftsregister oder Genossenschaftsregister, in das sie eingetragen sind, und die entsprechende Registernummer,

Auch das ist wieder nur für „richtige“ kommerzielle Anbieter notwendig.

Die Absätze 5 und 6 dieses Paragraphen beziehen sich nur Sonderfälle zur Umsatzsteuer-ID und für Anbieter, welche ihre Seite auch beruflich nutzen und diesen Beruf mit einem Hochschulabschluss ausweisen können.

Ob Sie in ihrem Impressum auch eine Telefonnummer angeben müssen ist heftig umstritten und lag bereits vor dem Bundesgerichtshof, welcher dies an den Europäischen Gerichtshof weiterleitete.

13.5 Datenschutz und das TDDSG

Das letzte Thema dieses Kapitels ist gleichfalls für viele das schwierigste. Denn mal ganz ehrlich: Wissen Sie genau welche Daten ihre DS erfasst? Da hätten wir zum Beispiel das Webalizer-spk, die Protokolle und natürlich auch ihre eigene Webseite. Auch Fremd-Inhalte wie zum Beispiel Werbung von Google AdWords können Daten erfassen. Daher ist es wichtig, dass Sie sich dieses etwas längere Kapitel sorgfältig durchlesen!

Beginnen wir mit ihren Pflichten und somit §4 des Telemedienschutzgesetzes (TDDSG):

> *(1) Der Diensteanbieter hat den Nutzer zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke der Erhebung, Verarbeitung und Nutzung personenbezogener Daten sowie über die Verarbeitung seiner Daten in Staaten außerhalb des Anwendungsbereichs der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. EG Nr. L 281 S. 31) zu unterrichten, sofern eine solche Unterrichtung nicht bereits erfolgt ist. Bei automatisierten Verfahren, die eine spätere Identifizierung des Nutzers ermöglichen und eine Erhebung, Verarbeitung oder Nutzung personenbezogener Daten vorbereiten, ist der Nutzer zu Beginn dieses Verfahrens zu unterrichten. Der Inhalt der Unterrichtung muss für den Nutzer jederzeit abrufbar sein.*

Also muss sichergestellt werden, dass Nutzer vor der Inanspruchnahme eines Dienstes, auf die erfassten und verarbeiteten Daten hingewiesen wird und er diesen auch später jederzeit abrufen kann.

> *(2) Bietet der Diensteanbieter dem Nutzer die elektronische Einwilligung an, so hat er sicherzustellen, dass*
>
> *1. sie nur durch eine eindeutige und bewusste Handlung des Nutzers erfolgen kann,*

Das automatische Aktivieren einer entsprechenden Box ist also nicht gestattet!

> *2. die Einwilligung protokolliert wird und*
>
> *3. der Inhalt der Einwilligung jederzeit vom Nutzer abgerufen werden kann.*
>
> *(3) Der Diensteanbieter hat den Nutzer vor Erklärung seiner Einwilligung auf sein Recht auf jederzeitigen Widerruf mit Wirkung für die Zukunft hinzuweisen. Absatz 1 Satz 3 gilt entsprechend,*

Achten Sie darauf einen Link zu setzen, mit Hilfe dessen der Nutzer von der „Erlaubnis“ zurücktreten kann.

> *(4) Der Diensteanbieter hat durch technische und organisatorische Vorkehrungen sicherzustellen, dass*

1. der Nutzer seine Verbindung mit dem Diensteanbieter jederzeit abbrechen kann,

2. die anfallenden personenbezogenen Daten über den Ablauf des Zugriffs oder der sonstigen Nutzung unmittelbar nach deren Beendigung gelöscht oder gesperrt werden können,

3. der Nutzer Teledienste gegen Kenntnisnahme Dritter geschützt in Anspruch nehmen kann,

4, die personenbezogenen Daten über die Inanspruchnahme verschiedener Teledienste durch einen Nutzer getrennt verarbeitet werden können,

5. Daten nach § 6 Abs. 2 nur für Abrechnungszwecke und

6. Nutzerprofile nach § 6 Abs. 3 nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden können.

Die Liste bis hierher zeigt ihnen, auf was sSe alles achten sollten. Abschnitt 6 besagt außerdem insbesondere: Sie dürfen in Foren u.ä., Pseudonyme nicht mit realen Personen in Verbindung bringen.

An die Stelle der Löschung nach Nummer 2 tritt eine Sperrung, soweit einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen.

(5) Die Weitervermittlung zu einem anderen Diensteanbieter ist dem Nutzer anzuzeigen.

Weiterleitungen u.ä. auf Angebote Dritte sind anzukündigen.

(6) Der Diensteanbieter hat dem Nutzer die Inanspruchnahme von Telediensten und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeit zu informieren.

Sie müssen ihren Nutzer darauf hinweisen, dass er im Zweifel das Recht hat (insofern dies technisch möglich ist), die Nutzung bzw. die Bezahlung anonym oder unter Pseudonym zu verlangen.

(7) Der Diensteanbieter hat dem Nutzer auf Verlangen unentgeltlich und unverzüglich Auskunft über die zu seiner Person oder zu seinem Pseudonym gespeicherten Daten zu erteilen. Die Auskunft kann auf Verlangen des Nutzers auch elektronisch erteilt werden.

Dieser letzte Teil ist besonders wichtig. Auch Sie können mit diesem schnell in Kontakt kommen. So kann ein Nutzer Ihnen eine E-Mail schreiben in der er auffordert, die über ihn erfassten Daten herauszugeben.

§6 des TDDSG beschäftigt sich nun mit den Rechten, welche der Inhaber der Informationen besitzt. So dürfen Daten ohne Einwilligung erfasst werden, falls diese

> *erforderlich [sind], um die Inanspruchnahme von Telediensten zu ermöglichen und abzurechnen (Nutzungsdaten). [..]*

Um genau zu sehen, welche Daten davon explizit betroffen sind, ist ein Blick in das TDDSG hilfreich.

In Abschnitt 2 folgt dann eine „Ausnahme“, wenn man so will, zu §4, Absatz 1 Abschnitt 6 (Zusammenführen von erfassten Daten und eines Pseudonyms):

> *(2) Der Diensteanbieter darf Nutzungsdaten eines Nutzers über die Inanspruchnahme verschiedener Teledienste zusammenführen, soweit dies für Abrechnungszwecke mit dem Nutzer erforderlich ist.*

Absatz drei geht diesbezüglich sogar noch etwas weiter:

> *(3) Der Dienstsanbieter darf für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Teledienste Nutzungsprofile bei Verwendung von Pseudonymen erstellen, sofern der Nutzer dem nicht widerspricht. Der Diensteanbieter hat den Nutzer auf sein Widerspruchsrecht im Rahmen der Unterrichtung nach § 4 Abs. 1 hinzuweisen. Diese Nutzungsprofile dürfen nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden.*

Soviel zum TDDSG. Fehlt noch ein letzter Abschnitt um dieses Thema abzurunden:

13.6 Haftung für Links

Die Haftung für Link ist besonders umstritten. Wenn man die Gesetzeslage ganz einfach sieht, so besagt §9 Teledienstgesetz:

> *Diensteanbieter im Sinne der §§ 9 bis 11 sind nicht verpflichtet, die von ihnen übermittelten oder gespeicherten Informationen zu überwachen oder nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen.*

Somit würde ein Anbieter nicht haften, wenn er nicht explizite Kenntnis über einen Verstoß der entsprechenden Seite besitzt. Völlig überraschend gab es in der Vergangenheit verschiedene Gerichtsentscheidungen unter anderem des BGH, welche das genaue Gegenteil vermuten lassen. Bis heute hängt das Urteil in einem solchen Fall häufig vom Gericht und den genauen Begebenheiten ab. Grundsätzlich ist zu beachten:

- Kann dem Anbieter nachgewiesen werden, dass er vom rechtswidrigen Inhalt wusste, ist in jedem Fall ein Verstoß aufgetreten.
- Der Anbieter sollte einen Hinweis auf seiner Seite anbringen, dass er für Links auf externe Seiten nicht haftet. Derartige „Beispiel-Disclaimer“ gibt es im Internet zu Hauf. (u.a.: http://www.e-recht24.de/muster-disclaimer.htm)
- Überprüfen Sie aus eigenem Interesse regelmäßig den verlinkten Inhalt auf eventuelle Rechtsverstöße.

13.7 Urheberrecht

Ein altes Thema, das dennoch insbesondere von neueren Webseiten-Schreibern gerne missachtet wird, ist das Urheberrecht. Viele denken über ihr Handeln nur dann nach, wenn wirklich ein großer Copyright-Hinweis in Nähe des Textes zu finden ist. Doch die Realität sieht anders aus. In

Deutschland gibt es, nur um die Rechte der Eigentümer von Werken zu wahren, das Urheberrechtsgesetz. §1 UrhG drückt die Gültigkeit des gesamten Urheberrechts aus:

> *Die Urheber von Werken der Literatur, Wissenschaft und Kunst genießen für ihre Werke Schutz nach Maßgabe dieses Gesetzes.*

Doch, wie die Definition in Wikipedia bereits deutlich macht, hat auch das Copyright seine Grenzen:

> *Das **Urheberrecht** ist der Teil einer Rechtsordnung, der in einem Rechtssystem das Recht des **Urhebers an seinen Werken** (subjektives Urheberrecht) schützt (objektives Urheberrecht). Dieser Schutz berücksichtigt wirtschaftliche Interessen und Ideale des Urhebers am Werk, wird aber zur Wahrung der Interessen der Allgemeinheit eingeschränkt (**Schranken des Urheberrechts**, zum Beispiel **Zitatrecht und Privatkopie**).*

- *- de.wikipedia.org/wiki/Urheberrecht*

In den weiterführenden Texten finden sich u.a. die folgenden Einschränkungen:

- Verwendung innerhalb von Behörden
- Vorübergehende Vervielfältigung (Beispielsweise beim RAM im Computer/Caches in Google)
- Vervielfältigung zu Gunsten behinderter Menschen
- Kopien für den Gebrauch im Rahmen des Kirchengebrauchs und im Schulunterricht
- Berichterstattung in Medien
- Zitate in anderen Werken

Das Urheberrecht erstreckt sich aber auch auf Räume wie beispielsweise Foren-Beiträge. Für diese gilt allerdings, dass das Werk ein „schützenswertes Ausmaß“ erreichen muss. Kurzum: Es ist Vorsicht geboten, wenn fremder Inhalt auf eigenen Seiten, Schriftstücken oder wo auch immer verwendet wird.

Im Kontrast zum Urheberrecht gibt es die Möglichkeit dessen, was im englischen Sprachraum als „Copyleft“ bezeichnet wird. Man kann also bestimmte Rechte abgeben, um anderen Vorteile daraus zu schaffen. Als Beispiel dazu gelten unter anderem die GNU GPL- und Creative Commons-Lizenzen.

14 „Around the Corner“ oder kleine Randnotizen

Hier noch ein paar Kleinigkeiten welche mir im Alltagsgebrauch meiner DS aufgefallen sind und durchaus erwähnt werden sollten.

14.1 Skype und ein Webserver

Da ich auch gerne den Webserver der DS für eigene Webseiten verwende, ist bei mir Port 80 freigegeben und auf die entsprechende Adresse weitergeleitet. Nun installierte ich Skype um auch im Ausland mit meinem Laptop billig zu Telefonieren. Nachdem ich meine ersten Versuche unternommen hatte, bekam ich einen erschreckenden Anruf: Meine Seite sei offline. Ein kurzer Check mittels Browser und SSH konnte keine Fehlfunktion aufdecken. Im Intranet lief alles tadellos. Naheliegend war also ein Defekt im Router. Nach einem Neustart dessen war auch meine Seite wieder erreichbar. Später konnte ich das Problem auf Skype eingrenzen. Ein Blick in das Skype-Handbuch deckte auf, dass Skype Port 80/443 zur Kommunikation verwendet. Der Vorteil dabei ist simpel wie effektiv: Normale Proxy-Server können Skype nicht erkennen und blockieren. Eine reibungslose Nutzung ist damit trotz Schutzmaßnahmen beispielsweise am Arbeitsplatz sicher. Ob mein Problem nun Router-spezifisch oder doch woanders zu suchen ist, kann ich nicht mit Sicherheit sagen. Doch nach ein wenig Probieren fand ich die Einstellung in Skype, welche die Nutzung der Ports 80/443 unterband.

14.2 Wordpress, Joomla, Zimplit auf einer DS

Wir haben hier ja bereits das „CMS4DS“ besprochen. Doch ich möchte mich hier auch zu den anderen CMS ein wenig äußern. Wer nach einer Vollständigen Lösung sucht, wird schnell Joomla oder Wordpress verfallen. Doch ich möchte vorwarnen: Sämtliche Testseiten welche von den Herstellern angegeben werden, befinden sich auf sehr teuren Hochleistungs-Servern, welche mit einer kleinen PHP-Abfrage keine Probleme haben. Nun kommt eine DS bei zu viel PHP und Datenbank schnell ins Schwitzen. Somit erreichen Seitenzugriffe schnell mehrere Sekunden und enden teilweise sogar in einem Server-Timeout oder ähnlichem.

Wer stattdessen einen Ausweg sucht, sollte nach möglichst schlanken CMS Ausschau halten. Überzeugt hat mich dabei auf den ersten Blick Zimplit CMS. Sicherlich gibt es auch Alternativen, aber Zimplit gefällt, da es keine dynamischen Seiten generiert, sondern ganz normale html- und CSS-Dateien. Somit ist ein Aufruf schneller abgewickelt als es dynamisch überhaupt möglich ist.

Bild: Unter (cc)-Lizenz von „swanksalot“ (Flickr)

12. Andere Anwendungen

15 Andere Anwendungen auf der DS

15.1 Offizielle Anwendungen von Synology

Um die Anwendungsmöglichkeiten der eigenen Produkte weiter zu erhöhen, arbeitet Synology seit noch nicht sehr langer Zeit an eigenen Anwendungen, welche optional installiert werden können.

Zum derzeitigen Zeitpunkt sind folgende Anwendungen verfügbar:

15.1.1 Die Mail Station

Die Mail Station ist eine Weboberfläche (Roundcube) zu dem im DSM integrierten E-Mail-Server. Sie dient dem Empfang und Versenden von Mails. Wer seine Postfächer mittels POP3 über Roundcube abrufen lässt, und zum Versenden den SMTP-Server des Anbieters nutzt, kann in der Firewall daher die betroffenen Ports sperren um die Sicherheit zu erhöhen. Wichtig: Die in Mail Station/Roundcube getroffenen Einstellungen zu SMTP-Servern treffen nur auf diese zu und können nicht in Programmen wie Outlook oder Thunderbird verwendet werden. Wenn Mails an den SMTP-Server der DiskStation gehen, nutzen diese stets auch den DiskStation-Server und nicht eventuell dort konfigurierte Alternativen.

15.1.2 Das SqueezeCenter

Von Logitech entwickelt und als Open Source herausgegeben, stellt dieses Paket eine Alternative zur integrierten Audio Station und dem Medienserver dar.

15.1.3 Webalizer

Diese Anwendung zeichnet jeglichen Verkehr über Port 80 und alle weiteren Ports welche manuell zur Web Station hinzugefügt wurden, auf. Webalizer erstellt dann sehr detaillierte Informationen über das Verhalten von Nutzern ihrer Seite. Nach Monaten aufgebrochen präsentiert Webalizer die Aktivitäten ihrer Nutzer inkl. den Top Eingangs und Ausgangsseiten, sowie vielen anderen Informationen, welche helfen können, Server und Webseiten effektiver zu verwalten. Auch dieses Programm basiert auf der Arbeit einer Open-Source Gruppe und wurde von Synology in eine .spk-Datei gepackt.

15.1.4 Time Backup

Wie schon im Kapitel zu Backups erläutert, dient Time Backup einem Versionsorientierten Backup. Im Gegensatz zu anderen Backupmethoden behält es auch ältere Versionen ein und löscht nur kontrolliert diese älteren Datensätze. Im Notfall können über eine Art Zeitstrahl die Dokumente wiederhergestellt werden.

15.1.5 phpMyAdmin

Die beliebte SQL-Administration ist auch als Zusatzpaket verfügbar. Es ermöglicht das Anlegen, Bearbeiten und Löschen von SQL-Datenbanken, sowie viele weitere Detaileinstellungen.

15.1.6 VPN Center

Um den Fernzugriff weiter zu vereinfachen hat Synology auch eine VPN-Software im Programm. Sie ermöglicht Zugang via OpenVPN und PPTP. Der verbindende PC (bzw. Smartphone o.ä.) baut bei beiden Technologien eine Direktverbindung über ein virtuelles Netzwerk auf. Je nach Einstellungen wird daher der gesamte Netzwerkverkehr oder ein Teil des selbigen über dieses Netzwerk geleitet. Mit nur einer Portfreigabe im Router sind damit auf sehr sicheren Weg sämtliche Dienste zugänglich.

Mehr zu den Technologien sowie ihren Unterschieden gibt es in Kapitel 1.3.4. Basierend auf diesem Kapitel ist PPTP für Einsteiger empfehlenswert, OpenVPN bietet jedoch mehr Optionen und Sicherheit bei etwas höherem Einrichtungsaufwand.

Auch an dieser Stelle sei auf die deutsche Community-Übersetzung des Benutzerhandbuchs hingewiesen, die alle weiteren Fragen beantworten sollte und bei der Ersteinrichtung genaue Schritt-für-Schritt-Anleitungen bereitstellt.[88]

Innerhalb von VPN Center kann auch eingestellt werden, wer sich via VPN verbinden darf, da ab Werk jeder Nutzer vollen Zugang zur VPN-Schnittstelle erhält.

15.1.7 Syslog-Server

Um in komplexeren IT-Umgebungen den Überblick zu behalten, ist eine zentrale Verwaltung von Systemmeldungen sehr hilfreich. Bei Softwareproblemen sind diese Meldungen oft ein wichtiger Schlüssel zur Eingrenzung. Um die Protokolle verschiedener Anwendungen zu sammeln gibt es unter Linux den Syslog-Daemon und die Gegenseite des Netzwerks stellt Synology mit diesem Zusatzpaket bereit. Detaillierte Informationen zu Funktionsweise und Einrichtung gibt es im Kapitel 3.1.

Mehr Informationen und die Downloads für alle Synology-Anwendungen unter: http://www.synology.com/apps/packages.php?lang=deu
Ab DSM 3.2 können Anwendungen von Synology auch direkt über die Internetanbindung des Paket-Zentrum installiert werden.

15.2 3rd-Party-Anwendungen – Vor dem Modden!

Bevor ich mit irgendeiner Anleitung beginne, welche sich mit der Veränderung von Soft- oder Hardware befasst (ich werde mich allerdings auf Software beschränken), muss ich noch auf die „Nebenwirkungen“ hinweisen. **Weil jetzt Anwendungen von Dritten verwendet werden, übernimmt weder Synology noch der Autor dieses Textes keine Garantie für eventuelle Probleme. Daher ist alles auf absolut eigene Gefahr!** Solange wir bei der Software bleiben, sollte nach einem erneuern der Firmware alles wieder beim alten sein. Doch dieser Vorgang ist immer mit dem Verlust aller bisher gespeicherten Daten verbunden. Daher ist ein Backup vor dem Modden ein Muss.

Die DiskStation kann aber nicht von Anfang an richtig mit unseren Modifikationen umgehen. Daher hat itari das SPK-Paket „init_3rdparty“ geschrieben. Einmal dieses ausgeführt, wird das Linux entsprechend vorbereitet. Nun können wir weitere Anwendungen installieren.

[88] http://www.synology-forum.de/showthread.html?20936-Deutschsprachige-VPN-Anleitung-zu-VPN-Center

15.3 Community-Anwendungen mit Oberfläche als .spk-Paket nachinstallieren

Wer eine komplette und aktuelle Liste mit allen Anwendungen einsehen will, erhält diese in unserem Wiki[89].

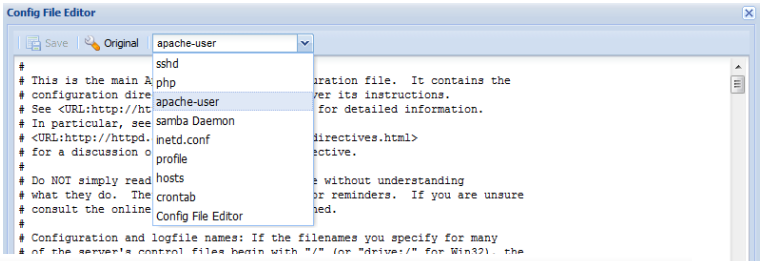
15.3.1 WICHTIG: Init_3rdparty

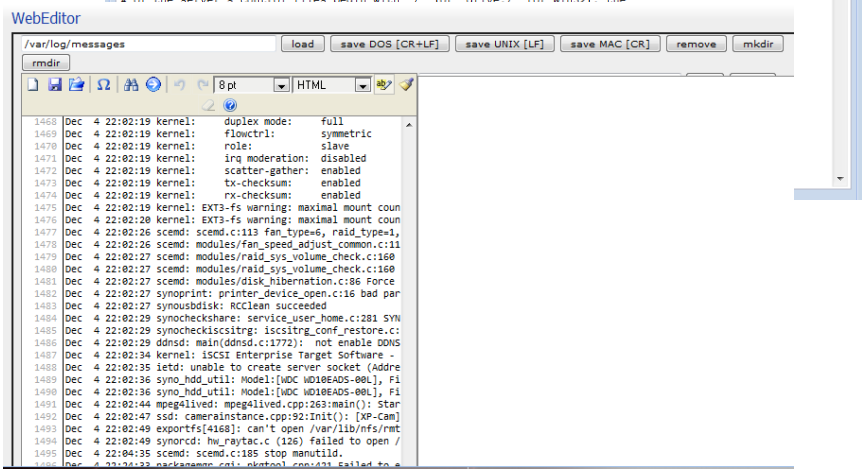
Bevor man die meisten zusätzlichen Anwendungen nutzen kann, wird ein Paket namens „init_3rdparty.spk“ vorausgesetzt, welches ein paar grundlegende Änderungen am Webserver durchführt, damit der DSM auch Zugriff auf weiterführende Bereiche des Systems hat. itari hat die Funktion des Pakets im Forum und im Wiki außerdem genauestens erklärt.

Für viele weitere Pakete ist auch ipkg unablässig, dessen Einsatz wir hier schon mehrfach erklärt haben (siehe u.a. Seite 136).

15.3.2 „webeditor“/“Config file editor“

Für Anfänger am nervigsten ist die Verwendung von Texteditoren auf CLI-Basis wie vi oder nano. Auch ich habe mich mit ihnen nie wirklich anfreunden können, doch zum Glück dauerte es nicht lange bis gleich zwei alternative Wege mit grafischer Oberfläche zur Verfügung standen.





Das deutlich einfachere von beiden ist der „Config file editor“ von Merty[90]. Die Oberfläche ist sehr einfach aufgebaut und die alte Vorlage kann schnell wiederhergestellt werden. Außerdem sind die Pfade zu den meisten Konfigurationsdateien schon eingespeichert. Umso schwerer gestaltet sich jedoch das Öffnen anderer Dateien.

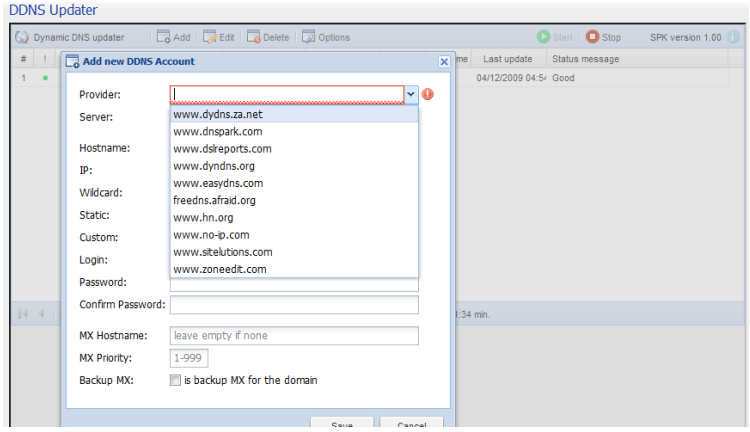
Für alle die gerne andere Dateien öffnen und mehr darin machen möchten, bietet sich itaris „webeditor“ an, der zwar von der Oberfläche deutlich komplexer wirkt, dafür aber auch eine größere Vielfalt an Funktionen und Optionen bereitstellt. Doch auch gefallen hier Komfortfunktionen wie Auswahl der Schriftgröße und des Formats, sowie Zeilennummern und ein „Suchen und Ersetzen“-Dialog zum Auffinden von gesuchten Zeichenfolgen.

Ein wenig weiter gehen außerdem zwei Anwendungen von itari die sich nur mit dem Samba beschäftigen, dessen Status abrufen und das Bearbeiten der Konfiguration vereinfachen.

89 http://www.synology-wiki.de/index.php/%C3%9Cbersicht_%C3%BCber_verf%C3%BCgbare_3rd-Party-Apps_aus_unserer_Community

90 http://www.mertymade.com/syno/

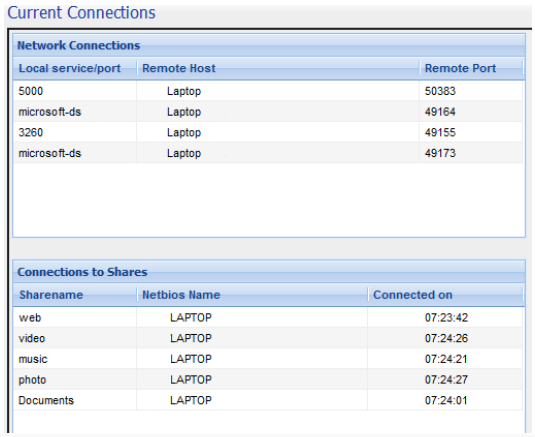
15.3.3 „DDNS Updater“



Aus einer großen Nachfrage heraus entstand dieses Projekt von QTip, in einer Zeit, als sich die Nachfragen zum Update mehrerer DDNS-Accounts immer mehr häuften. Bei den meisten hing das Limit bisher bei 2 Accounts, je ein Update durch Router und DS, bei anderen gar nur bei einem, wenn der Router kein DDNS beherrscht. Doch nun endlich gehören diese Sorgen der Vergangenheit an, denn dieses Paket kann unbegrenzt viele Accounts von vielen verschiedenen Anbietern updaten.

Das Programm ist zwar in Englisch geschrieben, doch die meisten Symbole sollten selbsterklärend sein und auch die meisten anderen Felder sind recht simpel. Nur eines sollte man nicht vergessen: Den „Start“-Knopf rechts oben drücken, damit der Hintergrundprozess anläuft.

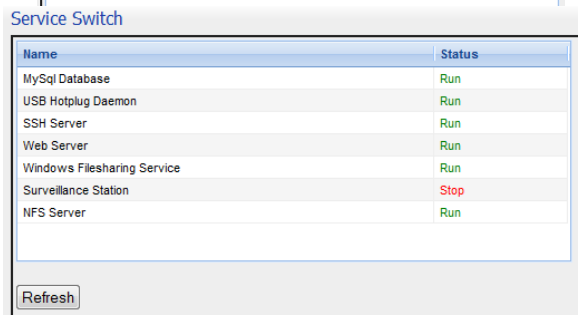
15.3.4 „Current Connection“



Häufige Fragen beschäftigen sich außerdem mit dem Anzeigen der momentan aktiven Verbindungen. Für einzelne Bereiche hat Synology dies bereits nachgereicht, für den Rest gibt es diese Anwendung von Merty.

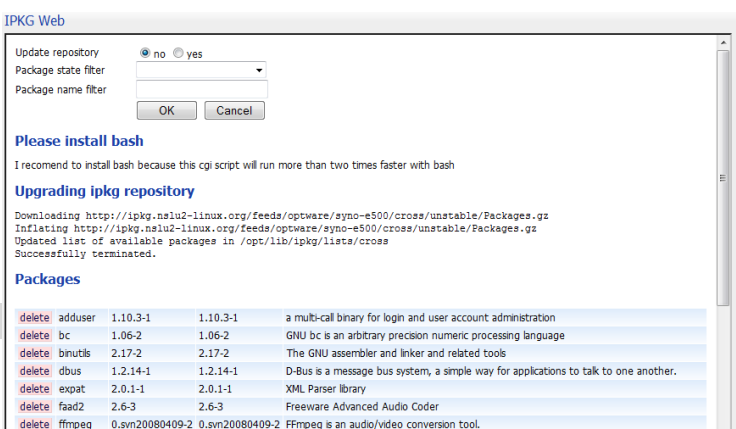
Das simple Interface zeigt zwei Tabellen, einen für sonstige Netzwerkverbindungen und eine für momentan verbundene Netzlaufwerke. Und ein „Refresh“-Button (Neu Laden) darf natürlich auch nicht fehlen.

15.3.5 „Service Switch“



Ein weiterer Eingriff in das System ist das Starten und Stoppen von Diensten. Ähnlich wie man das bei Windows vom Task-Manager kennt, kann auch diese Anwendung Dienste anhalten und wieder starten. Um das ganze etwas sicherer für Neulinge zu gestalten, sind nur Prozesse aufgeführt die nicht die Stabilität beeinträchtigen können. So findet sich der Backupprozess nicht darunter, da ein Anhalten während er arbeitet sehr riskant ist und meist zu Datenverlust führt. Auch der System-Webserver für den DSM wurde aus der Liste entfernt. Download[91] weitere Infos gibt es bei Merty, der auch dieses Paket sein eigen nennt.

15.3.6 „ipkg web“

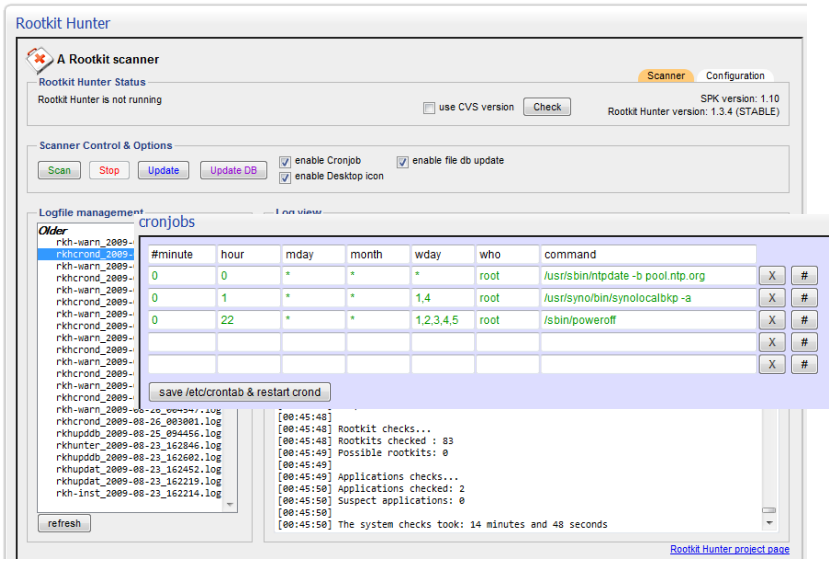


[91] http://www.mertymade.com/syno/

Viele Nutzer stolpern über das Installieren von ipkg-Anwendungen. Wer daher ipkg installiert hat und nicht immer auf das CLI gehen will, kann sich dieses Skript von noreway anschauen. Es installiert, aktualisiert und entfernt nach Belieben Pakete. Den Hinweis zu Bash kann man gezielt ignorieren. Sicher mag das Skript schneller sein, aber es geht auch prima ohne.

15.3.7 „Rootkit Hunter“

Viren für Linux gab es bisher noch sehr wenige. Doch wirklich problematisch sind Viren die NAS dazu verwenden sich selbst zu verbreiten. Woher also passende Gegenmittel nehmen? QTip hat sich einmal mit dem freien „Rootkit Hunter“ beschäftigt und dazu eine passende Oberfläche für den DSM geschrieben. Neben automatischen Updates und täglichen Scans ist auch eine Oberfläche zur manuellen Änderung der Konfigurationsdateien Inhalt des Pakets.

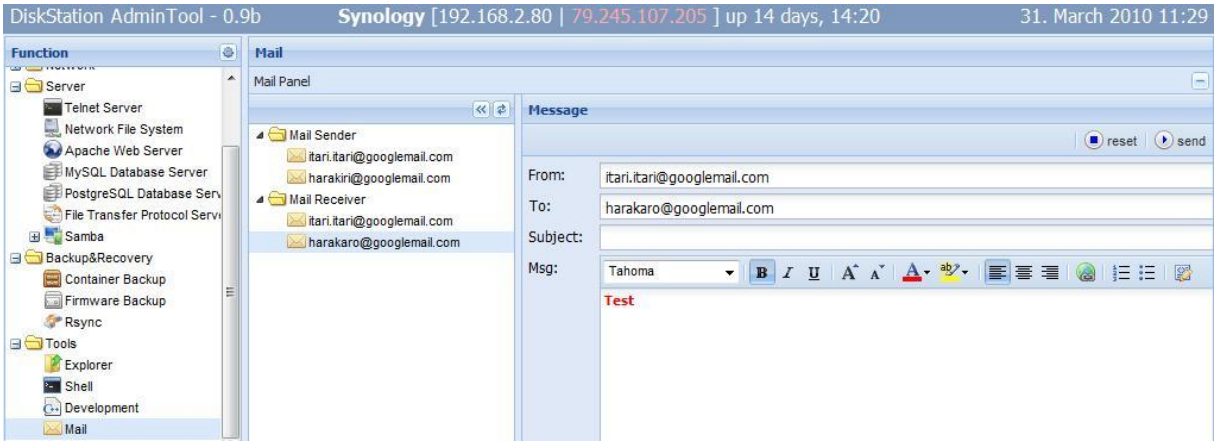


15.3.8 „cronjobs“

Was man unter Windows als „Aufgabenplaner“ abrufen kann, nennt sich in der Linux-Welt „cronjobs“. Die Rede ist vom Zeitgesteuerten ausführen von Skripten und Anwendungen. Eigene cronjobs sind zwar schnell definiert, doch deren Verwaltung und Überprüfung auf Schreibfehler nehmen viel Zeit in Anspruch. itari und ag_bg haben sich daher mit einem spk zur übersichtlichen Darstellung beschäftigt. Etwas technisches Verständnis über die Arbeitsweise dieser „jobs“ ist aber dennoch von Nöten.

15.3.9 „Admin Tool“

Als letzte Anwendung nun noch DAS Tool für Linux- und Modding-Interessierte. Itari hat alles was zum Modding nötig ist in eine einzige Anwendung gepackt: AdmintTool. Ich möchte hier gar nicht sämtliche Features aufzählen, denn das würde den Rahmen sprengen. Alles was im Modding-Bereich nötig ist kann dort mit wenigen Klicks geöffnet und geändert werden. Doch für mehr Details gibt es extra das Kapitel 15.6.



http://www.synology-wiki.de/index.php/Admin_Tool

Ich möchte das Kapitel über Anwendungen aus der Community damit erst einmal schließen, wohlwissend dass es noch viele weitere Pakete gibt die man hier nennen könnte, wie einen vollständigen DHCP-Server oder eine Oberfläche zum Steuern der Lichter an der Frontseite namens „Automate“ von itari.

15.4 Eigene Programme compilen

Auch ich werde mit alten Traditionen hier nicht brechen. Denn in jedem Buch über Programmiersprachen bildet ein simples Programm den Anfang, welches "Hello World" ausgibt. In C ist dies recht schnell geschrieben. Bereits hier sei angemerkt: Ich möchte und werde hier keine Programmiersprache erläutern, sondern nur wie eben jene C/C++Codes für eine DS erstellt werden können.

Doch genug dazu. Besagtes Test-Programm kann mit dem Editor der Wahl geschrieben und als "hello.c" gespeichert werden:

```
#include <stdio.h>
int main()
       {
       printf("Hello World\n");
       return 0;
       }
```

15.4.1 Das Compilen

Um einen Code für eine bestimmte Architektur zu erstellen gibt es in der Regel zwei Wege. Der erste ist das Erstellen über eine spezielle Toolchain, welche meist der Hersteller des Geräts anbietet. Oder aber man installiert auf dem Zielgerät einen bereits dafür angepassten Compiler. Wenn ein Linux auf dem Zielgerät läuft, ist es gut möglich, dass schon einer vorinstalliert ist oder sich leicht nachinstallieren lässt.

15.4.2 Compilen auf der DS

Auf der DS ist leider kein Compiler vorinstalliert. Der Weg führt hier stattdessen über ipkg, welches ohnehin zur Grundausstattung jedes Modders gehört. ipkg sollte auf Nachfrage folgendes melden:

```
DiskStation> ipkg list | grep gcc

gcc - 3.4.6-5 - The GNU Compiler Collection
```

Ein einfaches

```
ipkg install gcc
```

… sollte den GCC-Compiler inklusive dessen zusätzlich benötigten Paketen ohne Murren installieren und konfigurieren:

```
Installing gcc (3.4.6-5) to root...
Downloading http://ipkg.nslu2-linux.org/...
Installing binutils (2.17-2) to root...
Downloading http://ipkg.nslu2-linux.org/...
Installing libc-dev (2.3.4-5) to root...
Downloading http://ipkg.nslu2-linux.org/...
Installing libnsl (2.3.4-4) to root...
Downloading http://ipkg.nslu2-linux.org/...
Configuring binutils
```

```
update-alternatives: Linking //opt/bin/strings to /opt/bin/binutils-strings
Configuring gcc
Configuring libc-dev
Configuring libnsl
Successfully terminated.
```

(Links gekürzt)

Nun muss noch die Projektdatei „hello world.c“ auf die DS verschoben werden. In meinem Beispiel auf /volume1/Documents/hello (also in einen Unterordner des normalen „Documents“-Ordner den ich über den DSM erstellt habe).

An dieser Stelle möchte ich noch kurz etwas zu „man“ sagen. Die Linux-Benutzer unter den Lesern werden eventuell wissen, dass „man [programm]“ eine recht ausführliche Hilfe zu einem genannten Programm darbietet. Auf einer DS sind diese nicht vorinstalliert, aber eigentlich noch viel hilfreicher als auf GUI-basierten Systemen. Wer daher die ausführliche Hilfe nutzen möchte, kann diese über „ipkg install man-pages“ nachinstallieren. Dieses Paket enthält noch einige Verweise zu anderen Programmen welche automatisch mit installiert werden.

Doch nun zur eigentlichen Arbeit. Es geht in der Konsole weiter. Nach einem „cd“ in das entsprechende Verzeichnis mit unserer Quelldatei starten wir GCC:

```
DiskStation> gcc -Wall "hello world.c" -o hello
hello world.c:7:3: warning: no newline at end of file
```

Entschlüsseln wir einmal diese Ausgabe:

- gcc: ruft den Compiler auf
- -Wall: Diese Option aktiviert die erweiterten Compiler-Meldungen. Es wird dringend empfohlen diese Option zu nutzen, um Fehlern im Quelltext auf die Spur zu kommen.
- „hello world.c“: Hier wird die Quelldatei angegeben, welche meist auf .c endet. Die Anführungsstriche sind nur notwendig, da der Dateiname eine Leerstelle enthält. Sonst wäre hier auch eine Angabe ohne möglich.
- -o hello: Diese Option gibt an, wie die Ausgabedatei heißen soll. Sie ist optional, da sonst auf Standardwerte zurückgegriffen wird. Die Datei sollte keine Endung besitzen. Da es sich um ein zusammenhängendes Wort ohne Leerzeichen handelt, sind Anführungsstriche wie oben nicht notwendig.

Die darauf folgende Zeile ist eine kleine, nicht unbedingt wichtige Meldung. Sie weist auf ein Syntaxproblem hin, welches jedoch übergangen werden kann. Erzeugt wird sie durch die –Wall Option. Wenn es allerdings wichtigere Probleme gibt, so ist –Wall ein guter Helfer.

Die fertige Datei welche nun im binären Format vorliegt, also nicht wieder in ihre Programmiersprache zerlegt werden kann, ist ausführbar:

```
DiskStation> ./hello
Hello World
```

Die erste Zeile ruft die Datei „hello“ im momentanen („./“) Verzeichnis auf. Da unser Programm nur eine kurze Zeile Text ausgibt tut sich danach auch nicht mehr.

Mehr Informationen zur Arbeitsweise gibt es unter der man-Seite von gcc („man gcc“ auf der Konsole) sowie an vielen Stellen im Netz.[92]

15.4.3 Compilen mit der Toolchain

Wer sich nicht die Mühe machen möchte, auf dem Zielgerät einen Compiler einzurichten, der kann die bereits angesprochene Toolchain[93] nutzen. Leider ist das Cross-Compiling eine Wissenschaft für sich. Wer dennoch einen Versuch wagen möchte, sollte sich den „3rd-Party Apps Integration Guide“ zu Gemüte führen. Dort ist der komplette Prozess vom Herunterladen der Toolchain bis zum Integrieren in den DSM beschrieben. Ich würde hier aber den Rahmen sprengen wenn ich mich damit auseinander setzen würde.

Den Guide gibt es ebenfalls auf der Seite von Synology[94].

15.5 Integration in den DSM

Doch mit dem compilen ist es in der Regel nicht getan. Denn der Nutzer müsste nun immer noch auf das CLI zugreifen und den Kommando zum Starten manuell absetzen. Synology nutzt zur Interaktion den DSM und öffnet ihn nun auch gegenüber anderen Entwicklern.

Zusätzlich zu einer Integration in den DSM soll der Nutzer natürlich auch die Installation möglichst einfach bewältigen können. Dazu hat Synology ein eigenes Paketmanagement geschaffen. Diese SPK-Dateien enthalten alles dazu Notwendige. Doch eines nach dem anderen.

15.5.1 application.cfg

Die Integration in den DSM selbst läuft über eine Datei namens application.cfg welche die entsprechenden Parameter enthält. Der von Synology vorgegebene Pfad lautet **/usr/syno/synoman/webman/3rdparty/**. Erstellen Sie dort einen Unterordner der den Namen ihrer Anwendung trägt. In diesen Unterordner speichern Sie schließlich die Datei „application.cfg“ als einfache Textdatei. Auch sämtliche anderen Dateien wie Bilder gehören hier hin.

Nun muss diese Datei bearbeitet werden. Der Inhalt setzt sich aus folgenden Zeilen zusammen:

text = [Name] – [Name] muss hierbei durch eine Textzeile ersetzt werden die später im DSM als Bezeichnung für diese Anwendung stehen soll. Beispiel: *text = meineapp*

Lokalisierung, also die Anpassung an mehrere Sprachen, ist auch für Synology kein Fremdwort und kann über weitere Zeilen realisiert werden. Doch text zu ersetzen ist keine gute Idee, da der DSM bei einer nicht definierten Sprache nicht weiß was er machen soll. Daher sollten diese Spracherweiterungen nur zusätzlich und nicht ausschließlich genutzt werden.

Zur Lokalisierung wird ein Suffix verwendet. Die genauen Kürzel für jede Sprache lassen sich hier finden: */usr/syno/synoman/webman/texts/*

Ein Beispiel für Französisch (fre) würde so aussehen:
text_fre = monapp

[92] Offizielle Seite von gcc: http://gcc.gnu.org/
[93] Bei Synology zu finden unter http://sourceforge.net/projects/dsgpl/files/ im Ordner „Toolchain“. Auf dieser Seite gibt es für interessierte außerdem die Open-Source Kernkomponenten des angepassten Busybox-Linux.
[94] Synology-Webseite für „3rd-Party Entwickler“: http://www.synology.com/enu/support/3rd-party_application_integration.php

description = [Beschreibung] – Wobei [Beschreibung] durch eine kurze Erläuterung ihrer Anwendung zu ersetzen. Sie wird unter anderem dann angezeigt, wenn der Nutzer über dem Eintrag bleibt und ein „MouseOver“ ausgelöst wird sowie bei Nutzung der integrierten Suchfunktion des DSM.

Wiederum ist eine Lokalisierung über einen Suffix möglich. Beispiele:

description = kleine Anwendung
description_fre = petit app

Auch wenn man eigentlich mehr angeben sollte, ist hier der offizielle „Benötigt“-Teil beendet. Die folgenden Angaben sind daher optional, jedoch stark empfehlenswert.

icon_16 = [Pfad] – Um ein kleines Icon im DSM neben dem Namen der Anwendung darzustellen wird mit diesem Parameter der vollständige Pfad (in [Pfad]) zu einer 16x16 Pixel großen .PNG-Datei angegeben. Aufgrund der eingeschränkten Berechtigungen muss diese Datei in einem Unterordner von /usr/syno/synoman/webman/3rdparty/[app]/ sein. Für eine Datei „icon.png“ im Unterordner „images“ einer Anwendung „myapp“ müsste der Parameter [Pfad] also so lauten: /usr/syno/synoman/webman/3rdparty/myapp/images/icon.png

icon_32 = [Pfad] – Identisch mit icon_16 außer, dass die Größe hier 32x32 Pixel betragen soll.

type = [type] – Type gibt an wie die Anwendung geöffnet werden soll. Zwei Parameter sind möglich: „embedded“ und „popup“. Bei embedded wird die Anwendung im DSM im mittleren großen Fenster geöffnet währen im Falle von popup ein eigenes Fenster geöffnet wird. Allerdings sollte man sich vergewissern das alle modernen Browser einen Popup-Blocker mitbringen und es so zu Problemen kommen kann. Ist type nicht angegeben, wird popup als Standard verwendet.

Kommen wir als nächstes zur URL der php oder html-Datei die angezeigt werden soll. Synology sieht hierfür 4 Angaben vor:

protocol = [Protokoll] – Hier sind zwei Werte möglich: http und https. Fehlt diese Angabe, wird das momentane Protokoll des DSM verwendet.

address = [Adresse] – Zur Anzeige einer Seite außerhalb des DSM kann eine andere Domain oder IP-Adresse genutzt werden. Standardmäßig ist dieser Wert identisch mit der Adresse unter der der Nutzer die Seite gerade aufgerufen hat, also die des DSM.

port = [Port] – Hier kann zusätzlich zu „address“ noch der Port zum Zugang gesetzt werden. Auch hier ist der Standardwert mit der der momentan aufgerufenen Adresse identisch.

path = [Pfad] – Hinter der Domain kann nun noch der genaue Pfad zur Datei angegeben werden.

Die URL setzt sich also zusammen aus: protocol://address:port/path

Befindet sich die anzuzeigende Datei auf der DS selbst kann hier auch der Pfad angegeben werden. So hat beispielsweise QTip für seine Anwendung „rootkit hunter“ folgende Werte gewählt:

```
text = Rootkit Hunter
description = Rootkit Hunter, a Rootkit scanner
icon_16 = rkhunter16.png
icon_32 = rkhunter32.png
type = embedded
path = /webman/3rdparty/rkhunter/rkhunter.php
```

Dieses Beispiel verdeutlicht die Verwendung der einzelnen Parameter recht gut. Wer weitere Beispiele sucht kann verfügbare spk-Pakete im Rückwärtsprozess gegenüber dem nächsten Abschnitt auseinander bauen und sich die dortigen Dateien ansehen.

Synology gibt als weiteren letzten Hinweis noch, dass die Datei im Format UTF-8 gespeichert sein sollte. Diese Einstellung finden Sie in jedem halbwegs modernen Editor.

Wer außerhalb des DSM dennoch auf die Authentifizierung zugreifen möchte findet entsprechende Anleitungen im „Integration Guide“ von Synology wie bereits oben genannt.

15.5.2 spk-Pakete zur Vereinfachung der Installation

Offiziell gibt es von Synology keine Informationen über den Aufbau dieser Pakete. Jedoch haben einige fleißige Nutzer bestehende Pakete auseinander genommen und stellen ihre Erkenntnisse anderen zur Verfügung. Auch ich werde mich auf derlei Quellen stütze[95]. Mit bereits existierenden, gleichnamigen Lösungen hat dieses Paketmanagement jedoch nichts zu tun.

Nach guter alter Linux-Manier ist spk selbst ein simples tar-Archiv. Unter Linux lässt es sich daher über das meist integrierte Kommando „tar“ (ent-) packen (tar –xvf *datei*). Unter Windows erledigt dies beispielsweise das äußerst empfehlenswerte Open-Source „7zip“[96].

Dieses Archiv enthält mehrere Dateien und Verzeichnisse, wobei die Groß- und Kleinschreibung beachtet werden muss. Für die Textdateien wird außerdem strengstens empfohlen keine Sonderzeichen zu verwenden, da es sonst zu Problemen kommen kann. Als Standard wird der ASCII-Zeichensatz verwendet.

Die nötigen Informationen für das Paketmanagement selbst sind in der Datei **„INFO“** zu finden. Ähnlich wie schon die „application.cfg“ kann sie verschiedene Angaben nach dem Muster *parameter=“wert“* enthalten, wobei die Anführungszeichen hier allerdings Pflicht sind und später dem Nutzer nicht angezeigt werden.

Besonders wichtig ist die allererste Angabe. Sie muss einmalig sein und darf nicht mit anderen Paketen in Konflikt stehen: package

Die Angabe der Version dient intern nur der Bestimmung von neu und alt, ist aber sonst eher untergeordnet wichtig: version

Der Entwickler/Autor des Pakets dient nur zur Information für den Nutzer: maintainer

Auch eine kleine Beschreibung für den Nutzer darf natürlich nicht fehlen: description

Spannender wird es schließlich wenn ein Paket aufgrund von speziell kompilierten Binärdaten nur auf einer Architektur ausgeführt werden darf. Genaue Werte sind hier nicht bekannt, nur einzelne Bruchstücke. „noarch“ wird verwendet wenn keine Einschränkung besteht. Weitere Möglichkeiten wären beispielsweise „arm“ oder „ppc“ in Anlehnung an verschiedene Rechnerarchitekturen, genaue Infos liegen hierzu aber leider nicht vor: arch

[95] Insbesondere folgende: http://forum.synology.com/enu/viewtopic.php?f=27&t=10807
[96] http://www.7-zip.org/, auch erhältlich als 64-Bit-Version

Falls die installierte Anwendung später nicht im DSM erscheint sondern über einen eigenen Port angesteuert wird kann dieser ebenfalls angegeben werden. Die Angabe eines genauen Pfades ist jedoch nicht möglich: adminport

Auch hier möchte ich abschließend auf QTips „rootkit hunter“ als Beispiel zurückgreifen:

```
package="rkhunter"
version="1.10"
description="Rootkit Hunter, a Rootkit scanner"
maintainer="QTip"
admin_port=""
arch="noarch"
```

Wenn weitere Dateien für die Installation benötigt werden wie beispielsweise Binärdaten, so können diese wiederum in einem Archiv namens „**package.tgz**“ gepackt werden. Während der Installation wird dieses Archiv automatisch entpackt.

Bleiben noch die eigentlichen Skripte die bei einer (De-) Installation sowie beim Ausführen und Beenden ausgeführt werden:

- postinst
- postuninst
- preinst
- preuninst
- start-stop-status

Alle diese Skripte müssen im Ordner „scripts“ mit genau diesen Namen gespeichert werden. „pre“ steht dabei für Skripte vor und „post“ für Skripte die nach der (De-) Installation ausgeführt werden sollen. Geben diese Skripte „0“ zurück, wird die Ausführung als „problemlos“ eingestuft, bei „1“ wird der Vorgang sofort abgebrochen.

Je nach Aktion werden dem Skript „start-stop-status“ verschiedene Parameter bei Aufruf übergeben welche diesem verdeutlichen sollen was zu tun ist. Drei Möglichkeiten existieren dabei momentan: „start“ wenn die Anwendung gestartet werden soll, „stop“ wenn sie beendet werden soll und „status“ wenn der Status des Pakets erfragt wird. Als Rückgabewert wird auch hier „0“ (alles ok/Skript läuft) oder 1 (Fehler/Skript läuft nicht) erwartet.

Diese kurze Einführung sollte den meisten genügen und einen ausreichenden Überblick über die Arbeitsweise des eigenen Paketmanagements liefern. Wer jedoch eigene Pakete erstellen möchte sollte sich noch deutlich stärker mit den Innereien und dem Verfahren der spk selbst auseinandersetzen.

Wer sich dennoch entscheidet eigene Anwendungen zu schreiben kann sich gerne an die deutsche und internationale Community wenden, wobei letztere zusätzlich auch von Synology sowie von internationalen Entwicklern besucht wird und daher wohl mit genaueren Informationen zu rechnen ist.

15.6 Allzweckwaffe AdminTool

Und wieder ein Kapitel über etwas, das itari der Community geschenkt hat. Doch handelt es sich auch hier um etwas, um das man nicht herum kommt wenn man sich genauer mit einer DiskStation beschäftigt. Das Ziel ist es, alles was sonst nur über die Kommandozeile erreichbar ist, abrufbar zu

machen und es auch soweit wie möglich bearbeiten zu können. Die momentan (während ich dies schreibe) aktuellste Version ist 0.99c.

Und das Beste: Es ist mal wieder alles Open Source.

15.6.1 Installation

Voraussetzung für das AdminTool ist init_3rdparty.spk in der aktuellsten. Es hat auch einen Grund warum ich dieses Kapitel ganz nach hinten gesetzt habe. Hier können viele Änderungen vorgenommen werden die vorher beschrieben wurden und es wird auch viel Wissen der vorigen Kapitel für die richtige Anwendung vorausgesetzt. Da wäre zum Beispiel direkt nach der Installation des Tools noch die Installation der empfohlenen[97] ipkg-Pakete.

Entweder macht man dies über die Kommandozeile, oder man geht im AdminTool auf „AdminTool Configuration“ und öffnet dort den Reiter „install_ipkg.sh“. Nun sollte der Button „execute …“ (ausführen) sichtbar sein. Ein Klick darauf und die Installation wird gestartet. Diese Pakete sind für den Betrieb nicht zwingend notwendig, jedoch sind viele Funktionen sonst nicht nutzbar. Das Standardsystem enthält nicht viele Tools um Platz zu sparen und so müssen diese erst nachinstalliert werden.

15.6.2 Die „Verpackung“ …

Auf dem Screenshot sind die verschiedenen Bereiche gut zu erkennen. Ganz oben befindet sich eine Informations-Liste welche regelmäßig aktualisiert wird. Wenn das der Fall ist, fehlen alle Informationen und es ist nur ein Hinweis sowie ein sich drehender Kreis aus Punkten sichtbar.

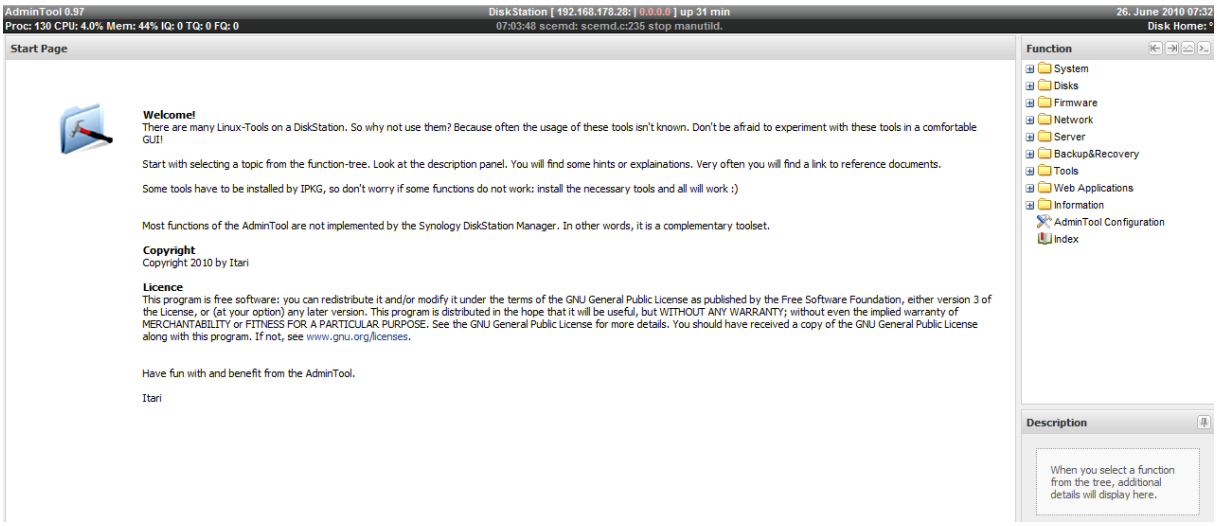
Aufgeführt sind dort: Version des AdminTool, Anzahl der Prozesse auf dem System sowie deren Auslastung von Arbeitsspeicher und Prozessor, Anzahl der Dateien in der Warteschlange der verschiedenen Multimedia-Dienste, Name der DiskStation sowie interne und externe IP, Zeit seit Systemstart, letzte Meldung im System-Log, Datum und Uhrzeit sowie die momentane Außentemperatur, ermittelt anhand einer ungefähren Ortsbestimmung des Internetanschlusses und einem Online-Wetterdienst.

So viel zum Kopf des Designs. Ich bin stets von links nach rechts und dann oben nach unten vorgegangen.

Die Navigation befindet sich standardmäßig an der rechten Seite, kann jedoch über die Pfeile neben dem Wort „Navigation“ auch nach links verschoben werden. Die anderen beiden Symbole daneben öffnen ein Fenster mit der Systemauslastung dargestellt als Graph sowie ein Shell-Fenster zur schnellen Eingabe von Kommandos. Darunter reihen sich fein säuberlich alle nur denkbaren Kategorien. Von Firmware und Synology-Anwendungen bis hin zu heiklen Punkten wie Backup und Festplatten ist praktisch alles vertreten.

Ein Klick auf die betroffene Kategorie erzeugt eine Tabelle welche die genauen Möglichkeiten jeder Option darstellt.

[97] Das Admintool lässt sich auch ohne diese benutzen, aber einige Funktionen sind eingeschränkt oder zeigen nur Fehlermeldungen ohne die ipkg-Tools.



15.6.3 … und der „Inhalt“

Ohne jetzt zu sehr auf die technischen Einzelheiten einzugehen möchte ich einmal kurz zeigen was sich genau hinter den einzelnen Kategorien verbirgt. Denn viele Dinge die einem das Leben als professioneller Anwender erleichtern können verstecken sich recht tief in den Namen der Kategorien und Seiten in englischer Sprache.

System – Hier wird von der Hardware (CPU, RAM, …) bis hin zum Linux alles beleuchtet was direkt auf oder mit der Hardware arbeitet. Dazu gehören auch die Dienste (Daemons), Prozesse und zeitgesteuerten Aktionen sowie die Statistiken zu „Gesundheit“ und Geschwindigkeit.

Disks – Ganz einfach formuliert gehört hier alles dazu, was Scheiben hat, Flash-Speicher wie SSDs einmal ausgenommen. Hier lässt sich einsehen und einstellen wie die Festplatten im System integriert sind und wie sie arbeiten. Dazu gehören auch Dateisysteme, Raids, SHR/LVM und S.M.A.R.T.-Werte.

Firmware – Alles was Synology selbst gemacht hat ist hier zusammengefasst. Unter anderem die Hardware (Kontrolle der LEDs am Gehäuse [98]), die Logdateien und die Einbindung von „Fremdanwendungen“ lassen sich hier einsehen und beeinflussen.

Network – Auch die technische Seite eines Netzwerkes bleibt nicht unbeleuchtet. So gehören zu dieser Kategorie DDNS, LAN-Schnittstellen, IP-Blockaden auf Systemebene und Porteinstellungen sowie entsprechende Statistiken um wenige zu nennen.

Server – Wenn man auch diese Kategorie ein wenig zusammenfasst, dann ist hier alles vertreten was die Kommunikation ermöglicht. Sei es auf Dateiebene (Samba), Webebene (Apache, Datenbanken) oder auf CLI-Ebene (Telnet).

Backup & Recovery – Ein häufiges Thema für ein NAS ist die Datensicherung. Im AdminTool lassen sich daher Backups anfertigen und kontrollieren. Insbesondere lässt sich hier rsync konfigurieren, der auch auf vielen anderen Linux-Systemen läuft und daher gern genutzt wird. Der DSM hält für ihn nur sehr spärliche Assistenten bereit.

[98] Passend zur Weihnachtszeit lässt sich die DS hier auch wie ein Weihnachtsbaum nutzen: Einfach alle LEDs auf „Blinken“ schalten. ☺

Security – Alles was helfen soll die Sicherheit zu erhöhen findet hier Platz. So u.a. Schnittstellen zur Automatischen Blockierung und zur Firewall.

Tools – Diese Kategorie vereint ein paar Tools die sonst im AdminTool verschwinden würden: Ein Dateibetrachter, ein Shell-Zugang, eine minimale C/C++-Entwicklungsumgebung ein Mail-Client und ein FTP-Client.

Web Applications – Diese Umschreibung enthält alles, was Synology an Anwendungen mitliefert, sei es Web Station, Photo Station etc.

Viel mehr gibt es zu diesem Tool gar nicht zu sagen, denn eine genaue Hilfe würde den Rahmen sprengen. Die meisten Dinge müssten Sie mit dem hier gewonnenen Vorwissen verstehen können. Und denken Sie daran: Erst Backup anfertigen, dann etwas ändern!

Nur ein kurzes Sahnehäubchen möchte ich Ihnen noch verraten: Klicken Sie doch mal auf die Kopfzeile des Tools.

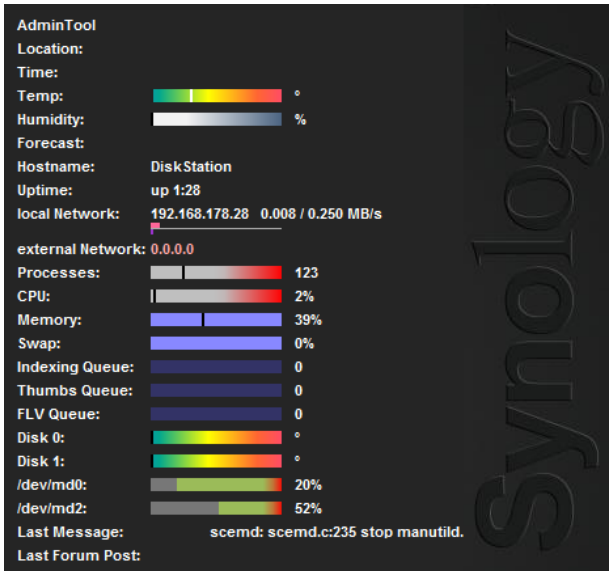


Bild: Unter (cc)-Lizenz von „Kristian D.“ („Flickr)

16 Nützliche Links

Die folgenden Links enthalten nützliche Informationen zum Thema Synology DiskStations, Linux-Entwicklung und allen anderen Dingen die hier besprochen wurden.

- Deutsches Synology-Forum: http://synology-forum.de
- Community Package Hub Projekt als Paketquelle: http://package.10trum.de/
- Internationales Forum: http://synology.com/forum
- Deutsches Synology-Wiki: http://synology-wiki.de
- Internationales Wiki: http://synology.com/wiki
- Synology Support inklusive Firmware-Updates, Kompatibilitätslisten und FAQ: http://synology.com/enu/support/index.php
- itaris kleine Seite zum Thema DiskStation und insbesondere deren Modifikationen: http://itari.pcip.de/ und http://itari.syno-ds.de/

Trotz sorgfältiger Prüfung der Links wird für deren Inhalt keine Haftung übernommen.

17 Index

I

J

K

L

M

N

O

P