# Einrichten der Synology DS1513+

1. Ins Netzwerk hängen
2. Reset-Knopf hinten drücken, 10 sec gedrückt halten währenddem vorne das Gerät eingeschaltet wird

(Damit wird die Netzwerk-Adresse freigegeben und er sucht sich eine IP über DHCP)

1. über http://find.synology.com die Station finden - ich musste das Programm Synology Assistant installieren, damit es klappte
2. Anmelden im Webbrowser, der durch den Synology Assistant oder manuell geöffnet wurde - nach dem Reset ist das Passwort leer
3. Über Systemsteuerung - Aktualisierung&Wiederherstellung - “Standard wiederherstellen” (oben rechts) das NAS auf seine Werkseinstellungen zurücksetzen
    - System startet neu, Webbrowser offen lassen
    - Im Webbrowser (evtl. aktualisieren) erscheint jetzt ein Dialog, um alles zurückzusetzen
    - alle Defaults übernehmen, Admin-Passwort vergeben, Servername vergeben und installieren lassen (Dauer: ca. 10 Minuten)
    - QuickConnect-Einrichtung überspringen
    - Keine statistischen Daten an Synology übermitteln
4. Es erscheint nun eine Frage, ob der Status überprüft werden soll
    - Ja und dahinter erscheint das Paketzentrum. Hier wird das Paket **MariaDB** installiert.
5. Systemsteuerung - Dateidienste starten
    - Arbeitsgruppen-Name ist VALAIR
    - Mac-Dienste deaktivieren
    - Übernehmen klicken
    - Netzwerk, oben “Netzwerk-Schnittstelle”: Lan1: Fixe IP vergeben gemäss IP-Sheet
        - Webbrowser wird automatisch auf neue Adresse umgeleitet
    - Terminal & SNMP:
        - ssh-Dienst aktivieren
    - Übernehmen klicken
    - Benachrichtigung einrichten und testen
6. Unter Systemsteuerung - Gemeinsamer Ordner folgende Freigaben einrichten:
    - transfer
    - sekretariat
    - verkauf
    - werkstatt
    - produkte
    - pbdh
    - gl
    - system
    - dbmedia
7. Benutzergruppen eröffnen
    - haas
    - gl
    - egl
    - verkauf
    - werkstatt
    - zugriff_0
    - zugriff_1
    - zugriff_5

    - zugriff_9
8. Benutzer eröffnen gemäss Passwortliste
9. Kopieren der Daten ab Harddisk
    - USB-Backup-Harddisk anhängen
    - putty starten und Verbindung mit Server herstellen, anmelden als admin
    - das USB-Laufwerk ist vermutlich unter /volumeUSB1/usbshare geladen worden
    - mit folgendem Befehl kann der gesamte Ordner-Inhalt in einen Ordner übertragen werden:

```
rsync -ah --progress /volumeUSB1/usbshare/server03/transfer/
/volume1/transfer/
rsync -ah --progress /volumeUSB1/usbshare/server03/sekretariat/
/volume1/sekretariat/
rsync -ah --progress /volumeUSB1/usbshare/server03/verkauf/
/volume1/verkauf/
rsync -ah --progress /volumeUSB1/usbshare/server03/werkstatt/
/volume1/werkstatt/
rsync -ah --progress /volumeUSB1/usbshare/server03/pbdh/ /volume1/pbdh/
rsync -ah --progress /volumeUSB1/usbshare/server03/gl/ /volume1/gl/
rsync -ah --progress /volumeUSB1/usbshare/server03/home/arueeger/
/volume1/homes/arueeger/
rsync -ah --progress /volumeUSB1/usbshare/server03/home/dhaas/
/volume1/homes/dhaas/
rsync -ah --progress /volumeUSB1/usbshare/server03/home/ksetz/
/volume1/homes/ksetz/
rsync -ah --progress /volumeUSB1/usbshare/server03/home/pbreguet/
/volume1/homes/pbreguet/
rsync -ah --progress /volumeUSB1/usbshare/server03/home/smartinez/
/volume1/homes/smartinez/
rsync -ah --progress /volumeUSB1/usbshare/server03/home/vdg/
/volume1/homes/vdg/
rsync -ah --progress /volumeUSB1/usbshare/server03/home/wallemann/
/volume1/homes/wallemann/
rsync -ah --progress /volumeUSB1/usbshare/server03/home/wbaumann/
/volume1/homes/wbaumann/
```

#### Einrichten des MariaDB-Servers

- Der DB-Server muss umkonfiguriert werden. Dazu muss ssh (putty) gestartet werden und wir müssen uns mit root anmelden.
- Anschliessend setzen wir die minimale Paketgrösse auf 64M, sonst können wir nicht mal die Bilder von

den Personen der Adress-Datenbank einlesen:

```
    cat /etc/mysql/my.cnf | sed 's/max_allowed_packet =
1M/max_allowed_packet = 64M/g' > /etc/mysql/my.new1
    cat /etc/mysql/my.new1 | sed 's/innodb_buffer_pool_size =
.*/innodb_buffer_pool_size = 1400M/g' > /etc/mysql/my.new2
```

```
cp /etc/mysql/my.cnf /etc/mysql/my.old
cp /etc/mysql/my.new2 /etc/mysql/my.cnf
rm /etc/mysql/my.new1
rm /etc/mysql/my.new2
/usr/share/mysql/mysql.server restart
```

Zudem:

```
skip-name-resolve
skip-host-cache und
lower_case_table_names=1
log-bin
binlog-format=MIXED
```

eintragen! Das ist die absolute minimale Konfiguration. Es könnten bessere Resultate erreicht werden, wenn ein Fachmann noch etwas optimieren würde... Nun ist noch der Zugriff auf die dbmedia-Verzeichnisse zu ermöglichen. Dazu wird der User mysql mittels vi in die Datei /etc/groups unter der Gruppe zugriff_0 eingetragen.

#### Rückspielen des MariaDB Backups

- Jeden Tag wird ein Fulltext-Backup der gesamten Datenbank inklusive aller Benutzer erstellt und im Freigabeordner system abgelegt. Diesen kann man mit einem einzigen Befehl zurückholen:
  - Ist noch kein root-Passwort in MariaDB festgelegt, dann so:

    ```
    mysql -uroot < /volume1/system/backup/mysql/full_dump.sql
    ```

  - sonst

    ```
    mysql -uroot -p < /volume1/system/backup/mysql/full_dump.sql
    ```

  - Das root-Passwort ist nun sofort gesetzt, da alle Passwörter aus dem Backup übernommen wurden.
  - Anschliessend muss die Datenbank auf den neusten MariaDB-Stand gebracht werden, falls bisher eine ältere Version eingesetzt wurde, mit

    ```
    /usr/bin/mysql_upgrade -uroot -p
    ```

#### Backup einrichten

- Um den freien Zugang zum Hauptserver zu erlangen, muss ein privater SSL-Key erstellt werden und dieser muss auf den anderen Server übertragen werden:

  ```
  cd ~
  haasdb-keygen -t rsa
  ```

- (alle Default-Werte übernehmen –> in ~/haasdb/ entstehen ein id_rsa.pub als öffentlicher Schlüssel und ein id_rsa als privater Schlüssel.

- Der öffentliche Schlüssel muss nun zum anderen Server übertragen werden und dort in die Datei /haasdb/authorized_keys eingetragen werden)

```
scp haasdb/id_rsa.pub root@portal.haas-ag.ch:
haasdb root@portal.haas-ag.ch
cat id_rsa.pub >> haasdb/authorized_keys
rm id_rsa.pub
exit
```

- Nun muss der eigene private Schlüssel noch geschützt werden:

```
chmod o-r-w-x haasdb/id_rsa
chmod g-r-w-x haasdb/id_rsa
```

- Wenn jetzt noch einmalhaasdb root@portal.haas-ag.ch aufgerufen wird, sollte das Login sofort und ohne Passwort möglich sein
- Nun muss das Backup-Script in /volume1/system überprüft werden in einem Editor /volume1/system/backup_haas.sh
- Wenn alles ok ist, kann das Script zeitgesteuert ausgeführt werden:
- Systemsteuerung - Aufgabenplaner - Erstellen - Benutzerdefiniertes Script
- Vorgang: Backup von Server XXX
- Benutzer: admin
- Script: /volume1/system/backup_haas.sh

#### Absicherung

- Systemsteuerung
  - Webdienste
    - Web Station aktivieren
    - HTTPS-Verbindung für Webdienste aktivieren
  - Zertifikate
    - Zertifikat erstellen (mehr oder weniger sinnvolle Angaben eingeben)
- Systemsteuerung
  - Netzwerk
    - DSM-Einstellungen:
      - Port 7245 und 7246 setzen
      - Umleitung auf HTTPS-Port erzwingen
  - Benutzer
    - Einstellungen
      - Kennwort-Regeln festlegen
- Systemsteuerung
  - Terminal und SNMP
    - haasdb-Port auf 2233 festlegen

#### MariaDB mit Zertifikat ausstatten und Benutzerkonten umstellen

Siehe auch Vorgehen nach Update MariaDB-Package

- Issuer-Zertifikat und Server-Zertifikat erstellen

```
    cd /etc/mysql
    [ -e certs ] && rm -Rf certs
    mkdir certs
    cd certs
    openssl genrsa 2048 > ca-key.pem
    openssl req -new -x509 -nodes -days 3600 \
         -key ca-key.pem -out ca-cert.pem -subj
'/C=CH/ST=Zuerich/L=Volketswil/O=Haas AG/CN=haas'
    openssl req -newkey rsa:2048 -days 3600 \
         -nodes -keyout server-key.pem -out server-req.pem  -subj
'/C=CH/ST=Zuerich/L=Volketswil/O=Haas AG/OU=haasdb/CN=haasdb'
    openssl rsa -in server-key.pem -out server-key.pem
    openssl x509 -req -in server-req.pem -days 3600 \
         -CA ca-cert.pem -CAkey ca-key.pem -set_serial 01 -out server-
cert.pem
    Die ca-cert.pem ist für die Clients bestimmt und wird nach
/volume1/transfer/Software/haasadmin kopiert:
    cp ca-cert.pem /volume1/transfer/Software/haasadmin/
    Ebenso wichtig ist es nun, die Zertifikate in die /etc/mysql/my.cnf
einzutragen, mit folgenden Zeilen:
ssl
ssl-ca = /etc/mysql/certs/ca-cert.pem
ssl-cert = /etc/mysql/certs/server-cert.pem
ssl-key = /etc/mysql/certs/server-key.pem
```

- Anschliessend unbedingt mysql neu starten:

```
/usr/share/mysql/mysql.server restart
```

- Nun werden die Zertifikate für alle Datenbank-User erstellt. Dazu verwenden wir die Tabelle personal als Referenz:

```
echo "#!/bin/sh" >/var/tmp/userlist.tmp
mysql -Nsr -uroot -p -Dhaas >>/var/tmp/userlist.tmp <<EOF
SELECT CONCAT(
'# ****** ', login_user, '\n',
'[ -e /volume1/homes/', login_user, '/haasdb ] && rm -Rf /volume1/homes/',
login_user, '/haasdb\n',
'mkdir /volume1/homes/', login_user, '/haasdb\n',
'openssl req -newkey rsa:2048 -days 3600 -nodes -keyout /volume1/homes/',
login_user,
'/haasdb/key.pem -out /volume1/homes/',
login_user,
'/haasdb/req.pem -subj \'/C=CH/ST=Zuerich/L=Volketswil/O=Haas AG Print
Finishing Systems & Solutions/OU=',
REPLACE(IFNULL(text_1, login_user), 'ü', 'ue'),
'/CN=', login_user, '\'\n',
'openssl rsa -in /volume1/homes/',
login_user,
'/haasdb/key.pem -out /volume1/homes/',
```

```
login_user,
'/haasdb/key.pem\n',
'openssl x509 -req -in /volume1/homes/',
login_user,
'/haasdb/req.pem -days 3600 -CA ca-cert.pem -CAkey ca-key.pem -set_serial 01
-out /volume1/homes/',
login_user,
'/haasdb/cert.pem\n',
'chown -R ', login_user, ':users /volume1/homes/', login_user, '/haasdb') \
FROM personal p join mysql.user u on u.user = p.login_user and u.host =
'192.168.1.%' WHERE p.inaktiv = 0 AND p.gruppe_jn = 0 and p.login_user =
'lager';
EOF

chmod u+x /var/tmp/userlist.tmp
/var/tmp/userlist.tmp
rm /var/tmp/userlist.tmp
```

- Nun werden die Benutzer umgestellt. Bisher meldete sich xyz mit einem Password pw_xyz an. Neu darf er sich, sofern er aus dem internen Netz kommt und SSL-zertifiziert ist, ohne Passwort anmelden. Kommt er jedoch von aussen, dann soll er sich mit dem bisherigen Passwort anmelden. Ohne SSL-Zertifikat darf er sich hingegen gar nie mehr anmelden.
- Dazu müssen zuerst die Benutzer von % auf 192.168.1.% umgestellt werden mit

```
mysql -uroot -p -e"update mysql.user set host = '192.168.1.%' where host =
'%';
mysql -Nsr -uroot -p -Dhaas >/var/tmp/userlist.tmp <<EOF
    SELECT CONCAT(
    'GRANT SELECT, INSERT, UPDATE, DELETE, EXECUTE ON haas.* TO \'',
    login_user,
    '\'@\'%\' REQUIRE Subject \'/C=CH/ST=Zuerich/L=Volketswil/O=Haas AG
Print Finishing Systems & Solutions/OU=',
    IFNULL(text_1, login_user),
    '/CN=', login_user, '\' AND ISSUER
\'/C=CH/ST=Zuerich/L=Volketswil/O=Haas AG/CN=haas\';\n',
    'set password for \'', login_user, '\'@\'%\' = \'', password, '\';\n',
    'GRANT USAGE ON haas.* TO \'',
    login_user,
    '\'@\'192.168.1.%\' REQUIRE Subject
\'/C=CH/ST=Zuerich/L=Volketswil/O=Haas AG Print Finishing Systems &
Solutions/OU=',
    REPLACE(IFNULL(text_1, login_user), 'ü', 'ue'),
    '/CN=', login_user, '\' AND ISSUER
\'/C=CH/ST=Zuerich/L=Volketswil/O=Haas AG/CN=haas\';\n',
    'set password for \'', login_user, '\'@\'192.168.1.%\' = \'\';\n') \
    FROM personal p join mysql.user u on u.user = p.login_user and u.host =
'192.168.1.%' WHERE p.inaktiv = 0 AND p.gruppe_jn = 0;
EOF

mysql -uroot -p </var/tmp/userlist.tmp
```

```
rm /var/tmp/userlist.tmp
```

#### IPKG installieren

Mit IPKG können verschiedene von Synology nicht selber unterstützte Packages installiert werden. Für die Duplikate-Suche haben wir das Paket fdupes installiert. Dazu haben wir folgende Anleitung im Netz befolgt: https://salmanzg.wordpress.com/2012/11/27/duplicate-files-synology-nas/

#### Mailserver installieren

Damit die Datenbank nächtlich ihre E-Mails rumschicken kann (Check-e-Mails etc.) muss der Mailserver installiert sein. Dazu das Package Mail-Server installieren und anschliessend einen Hostnamen (server04.haas-ag.ch) eintragen.