Einrichten der Synology DS1515+

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. Package MailServer installieren
7. Unter Applikationen - MailServer - SMTP folgende Einstellungen vornehmen:
    - SMTP aktivieren: ja
    - Hostname: dsm01.valair.ch
    - Rest alles default belassen
    - Damit werden die Mails (z.B. check_auftraege, siehe weiter unten) verschickt
8. Unter Systemsteuerung - Gemeinsamer Ordner folgende Freigaben einrichten:
    - daten
    - system
9. Benutzergruppen eröffnen
    - zugriff_0
    - zugriff_1
    - zugriff_5
    - zugriff_9
10. Benutzer eröffnen gemäss Passwortliste
11. Kopieren der Daten ab Harddisk oder altem Server

Einrichten des MariaDB-Servers

- MariaDB Package installieren
- In der Package-Einrichtung den Port auf 4306 setzen (statt 3306)
- Der DB-Server muss umkonfiguriert werden. Dazu muss ssh (putty) gestartet werden und wir müssen uns mit root anmelden.
- Die normale Konfiguration eines MariaDB-Servers liegt in `/etc/mysql/my.cnf`. Diese Datei rühren wir aber nicht an, denn das Synology MariaDB Package stellt für eigene Anpassungen daran die Datei `/var/packages/MariaDB/etc/my.cnf` zur Verfügung. Existiert eine solche Datei, wird sie eingelesen und erhält Vorrang über die Einstellungen in `/etc/my.cnf`.
- Wir erstellen also mit `vi /var/packages/MariaDB/etc/my.cnf` die Datei und füllen sie mit folgendem Inhalt:

```
[client]
port=4306
default-character-set=utf8mb4

[mysqld]
port = 4306
socket = /run/mysqld/mysqld.sock
collation-server=utf8mb4_general_ci
character-set-server=utf8mb4
skip-name-resolve
skip-host-cache
lower_case_table_names=1
group_concat_max_len=50000000

max_allowed_packet = 64M
innodb_buffer_pool_size = 2800M

event_scheduler=ON


ssl
ssl-ca = /var/packages/MariaDB/etc/ca-cert.pem
ssl-cert = /var/packages/MariaDB/etc/server-cert.pem
ssl-key = /var/packages/MariaDB/etc/server-key.pem
```

Rückspielen des MariaDB Backups

- Jeden Tag werden alle Datenbanken in ein Dump-File exportiert. Jedes wird mit dem Datenbanknamen und dem Monats-Tag gekennzeichnet; der Stand am Monatsende mit dem ganzen Datum.
- Das Backup wird durch das Script /volume1/system/backup/mysql/dump_databases.sh durchgeführt. Es ist in der Systemsteuerung des DSM unter Aufgabenplanung eingetragen und wird jeden Abend um 21:30 Uhr gestartet
    - 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 ~
ssh-keygen -t rsa
```

- (alle Default-Werte übernehmen –> in ~/.ssh/ 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 /.ssh/authorized_keys eingetragen werden)

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

- Nun muss der eigene private Schlüssel noch geschützt werden:

```
chmod o-r-w-x .ssh/id_rsa
chmod g-r-w-x .ssh/id_rsa
```

- Wenn jetzt noch einmal ssh root@valair.casaluna.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_valair.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_valair.sh

MariaDB mit Zertifikat ausstatten

Damit die Kommunikation zwischen Client und MySQL-Server verschlüsselt wird, generieren wir ein Zertifikat und installieren es auf dem Server. Das ca-cert.pem, das Zertifikat der Ausgabestelle, verteilen wir dann über die Start-Scripts auf die Clients, die Zugriff auf die Datenbank benötigen. Dann können wir die Benutzer umstellen und bei ihnen mittels REQUIRE ISSUER = ... sicherstellen, dass die Verbindung auch tatsächlich verschlüsselt wird.

- Issuer-Zertifikat und Server-Zertifikat erstellen

```
    cd /volume1/system
    [ -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=Thurgau/L=Sitterdorf/O=Valair AG/CN=valair'
    openssl req -newkey rsa:2048 -days 3600 \
         -nodes -keyout server-key.pem -out server-req.pem  -subj
'/C=CH/ST=Thurgau/L=Sitterdorf/O=Valair
AG/OU=valairdb/CN=valair.casaluna.ch'
    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/daten/44 IT/9/flightops kopiert:

```
    cp ca-cert.pem /volume1/daten/44\ IT/9/flightops/
```

- Ebenso wichtig ist es nun, die Zertifikate in die `/var/packages/MariaDB/etc/my.cnf` einzutragen, mit folgenden Zeilen:

```
ssl
ssl-ca = /volume1/system/certs/ca-cert.pem
ssl-cert = /volume1/system/certs/server-cert.pem
ssl-key = /volume1/system/certs/server-key.pem
```

- Anschliessend unbedingt mysql neu starten:

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

```
  * Nun werden die Benutzer umgestellt. Dazu muss mit REQUIRE ISSUER
verlangt werden, dass sie das dbuser-Zertifikat zeigen.
```

Weitere Augaben

In der Systemsteuerung, Aufgabenplanung sind noch zwei weitere Jobs aufzunehmen:

- /volume1/system/check_auftraege.sh: Sendet morgens 07:30 eine E-Mail, wenn Auftragstotale

nicht übereinstimmen
- /volume1/system/calc_lfz_status.sh: Rechnet morgens um 03:00 den Luftfahrzeugstatus für alle Helikopter neu