Zusätzlich Tipps und Informationen

Sollten sie SQLite anstelle von MySQL nutzen wollen, können sie die überflüssigen Pakete mit folgenden Befehlen deinstallieren:

sudo apt-get purge mysql-server mysql-client php5-mysql phpmyadmin -y
sudo apt-get autoremove --purge -y
sudo apt-get autoclean

Möchten sie einen zusätzlichen Benutzer einrichten, gehen sie wie folgt vor:

Mit „sudo -i“ erlangen sie während des gesamten Vorgangs Root-Rechte. In die vorhergehende Sitzung gelangen sie mit „exit“

„adduser username“	legt neuen Benutzer an.
„passwd username“	dem Benutzer ein Passwort geben. (Blindeingabe)
„usermod -s /bin/bash username“	Standard-Bash zuweisen
„usermod -g users username“	Dem Benutzer die Hauptgruppe zuweisen.

Tip: mit „deluser –remove-home username wird ein Nutzer gelöscht.

Um Nextcloud zusätzlich zu beschleunigen empfiehlt es sich einen Memory Cache einzurichten. Dies ist recht einfach. Dazu muss nur eine neue Zeile in die config.php eingetragen werden.

Mit „sudo nano /var/www/nextcloud/config/config.php“ öffnen sie die Datei im Editor nano. Fügen sie vor der letzten Zeile „);“ folgendes ein:

'memcache.local' => '\OC\Memcache\APCu',

Speichern sie alles mit STRG+O und schließen danach den Editor.

Um einfach Dateien auf den Raspi schieben zu können ist eine Samba-Freigabe hilfreich. Samba lässt sich mit wenigen Befehlen installieren und einrichten.

Samba installieren:
„sudo apt-get update“
„sudo apt-get install samba samba-common smbclient“

Prüfen ob Samba läuft:
„sudo service smbd status“
„sudo service nmbd status“
Beide Dienste sollten laufen.

Grundkonfiguration des Samba Servers:
„sudo mv /etc/samba/smb.conf /etc/samba/smb.conf_alt“
„sudo nano /etc/samba/smb.conf“

In die neue smb.conf folgendes eintragen:

[global]
workgroup = WORKGROUP
security = user
encrypt passwords = yes

Mit STRG+O / Return /STRG+X speichern und nano beenden.

Mit „testparm“ prüfen ob die smb.conf OK ist.

Samba Dienste neu starten mit:
„sudo service smbd restart“
„sudo service nmbd restart“

Freigabe Verzeichnis (Hier befinden sich später alle Freigaben) erstellen:

„sudo mkdir /home/shares“

„sudo mkdir /home/shares/freigabe1
„sudo chown root:root /home/shares/freigabe1/ /root:users -> Gruppe Users
„sudo chmod 777 /home/shares/freigabe1/ /770 -> Gruppen 700 -> User)

Die Freigabe in die Samba Konfigurationsdatei eintragen:

„sudo nano /etc/samba/smb.conf

[Freigabe1]
comment = Testfreigabe1
path = /home/shares/freigabe1
read only = no

Mit STRG+O / Return /STRG+X speichern und nano beenden.

Samba Dienste neu starten mit:
„sudo service smbd restart“
„sudo service nmbd restart“

Samba Passwort für Benutzer einrichten:
„sudo smbpasswd -a pi“

Ab jetzt können sie die Freigabe nutzen.

Soll ein Raspberry ohne Display und Tastatur genutzt werden, müssen wir seine IP Adresse für die erste Einrichtung per SSH herausfinden.

Unter Linux können wir uns alle Raspi Mac-Adressen die im Netz verfügbar sind anzeigen lassen. Das können wir mit folgendem Befehl machen:

„ip n | grep „b8:27:eb“

Als Windowsnutzer bedienen wir uns eines Tricks (der auch mit Linux funktioniert (-b)).

Wir setzen ein Ping an die Broadcast-Adresse des Netzes ab (.255) und lassen uns danach den ARP-Cache ausgeben der eine Zuordnung von IP V4 Adressen zur MAC-Adresse enthält. Raspberrys haben eine MAC Adresse die mit „b8:27:eb“ anfängt.

„ping 192.168.xxx.255“
„arp -a“

Es gibt eine einfache Möglichkeit externe Festplatten bzw. USB Stick o.ä. in Nextcloud einzubinden. Dies funktioniert wie folgt:

Das Laufwerk sollte nach dem anstecken mit ext4 formatiert werden.

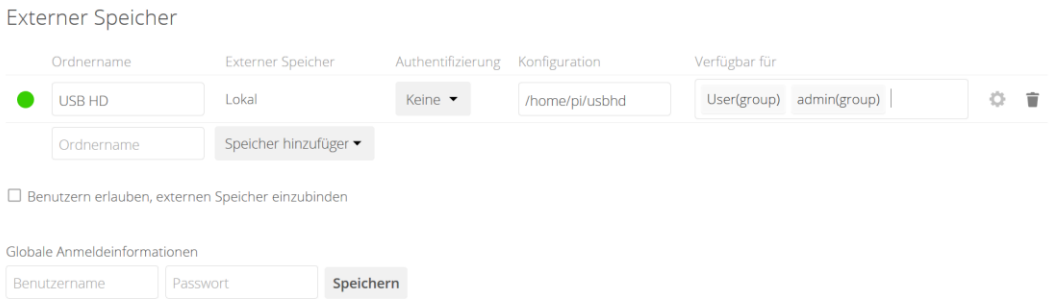
„sudo nano /boot/config.txt | Am Ende der Datei max_usb_current=1 einfügen.
„mkdir /home/pi/usbhd“ | Der Ordner in dem die HD gemountet wird.
„lsblk“ | Prüfen ob die HD erkannt wurde. (sda bzw. sda1)
„sudo mount -t auto /dev/sda1/ home/pi/usbhd“ | Festplatte mounten
„sudo chown -R www-data:www-data /home/pi/usbhd“ |Besitzer auf www-data ändern

Um die HD bei booten automatisch zu mounten:

„sudo nano /etc/fstab“
/dev/sda1 /home/pi/usbhd auto noatime 0 0 | Einfügen

Als Admin bei nextcloud anmelden.
Bei +Apps->Nicht aktiviert „External Storage support“ aktivieren.

Administration-> Externer Speicher



---

spdns DDNS Update Client installieren

Damit der Raspi aus dem Internet erreichbar ist, haben wir uns einen DynDNS Account erstellt und uns einen Domainnamen eingetragen. Damit nun der Raspi auch wirklich erreichbar ist, müssen wir dem DynDNS Anbieter unsere IP mitteilen. Das machen wir wie folgt:

„cd /home/pi/“
„wget http://my5cent.spdns.de/wp-content/uploads/2014/12/spdnsUpdater_bin.tar.gz“
„tar -zxvf spdnsUpdater_bin.tar.gz“
„sudo mv spdnsu.conf /etc/“
„sudo mkdir updater“
„sudo mv spdnsu updater/“
„sudo chmod u+x updater/spdnsu“
„sudo chown -R pi:pi /home/pi/updater/“
„rm spdnsUpdater_bin.tar.gz“

spdnsu.conf anpassen:

sudo nano /etc/spdnsu.conf

```
[HOST]
# URL for the Host to be update
# updateHost = update.spdns.de
host = host1.spdns.de
user = user1
pwd  = blah
isToken = 1
```

Hier die entsprechenden Werte eintragen.

Mit STRG+O / ENTER / STRG+X speichern und schließen.

Damit die Aktualisierung automatisch geschieht erstellen wir einen cronjob. In diesem Fall alle 10 Minuten.

„sudo crontab -e“

Dort fügen wir folgendes ein:

*/10 * * * * /home/pi/updater/spdnsu

Mit STRG+O / ENTER / STRG+X speichern und schließen.

Einen manuellen Aufruf zum Testen.
„./updater/spdnsu“

Die aktuelle IP-Adresse steht in /tmp/spdnsuIP.cnf
„cat /tmp/spdnsuIP.cnf“

Let’s Encrypt SSL Zertifikat erzeugen und installieren

Damit der Zugriff auf unsere Dateien auch verschlüsselt stattfinden kann, benötigen wir ein SSL Zertifikat. Grundsätzlich ist es möglich sich selbst ein Zertifikat auf dem Pi zu generieren. Der große Nachteil ist, dass diese Zertifikate trotzdem nicht als Vertrauenswürdig gelten und erst in Browser und Programme importiert werden müssen.

Wir erstellen uns stattdessen ein SSL Zertifikat bei Let’s Encrypt. Was genau Let’s Encrypt ist, von wem es unterstützt wird usw. kann man auf deren Website nachlesen. Diese Zertifikate werden von allen gängigen Browsern und Programmen als Vertrauenswürdig angesehen.

Wir gehen wie folgt vor:

„sudo a2enmod ssl“

„sudo a2enmod headers“

„sudo service apache2 restart“

„sudo apt-get install git -y“

„cd /etc“

„sudo git clone https://github.com/letsencrypt/letsencrypt“

„cd letsencrypt“

„sudo ./letsencrypt-auto“

Nach einer ganzen Weile müssen sie eine E-Mail-Adresse eingeben. Das ist wichtig. Diese benötigen sie zur Erneuerung des Zertifikats.

Dann müssen sie den Nutzungsbedingungen zustimmen. (A)

Jetzt können sie Wählen ob sie ihre Mail-Adresse der EFF mitteilen lassen wollen um auf dem Laufenden zu bleiben. (Ihre Entscheidung)

Dann wird nach dem Domainnamen gefragt. Hier müssen sie den Namen ohne http, www. o.ä. eingeben.

Nach einem kleinen Moment sollte das Zertifikat auf dem Raspi gespeichert werden.

Jetzt müssen sie nur noch eingeben wie der Zugriff erfolgen soll. Hier sollten sie unbedingt die sichere Variante wählen. Sonst haben sie zwar einen SSL Zugang, aber die Daten werden auch noch per http ausgeliefert.