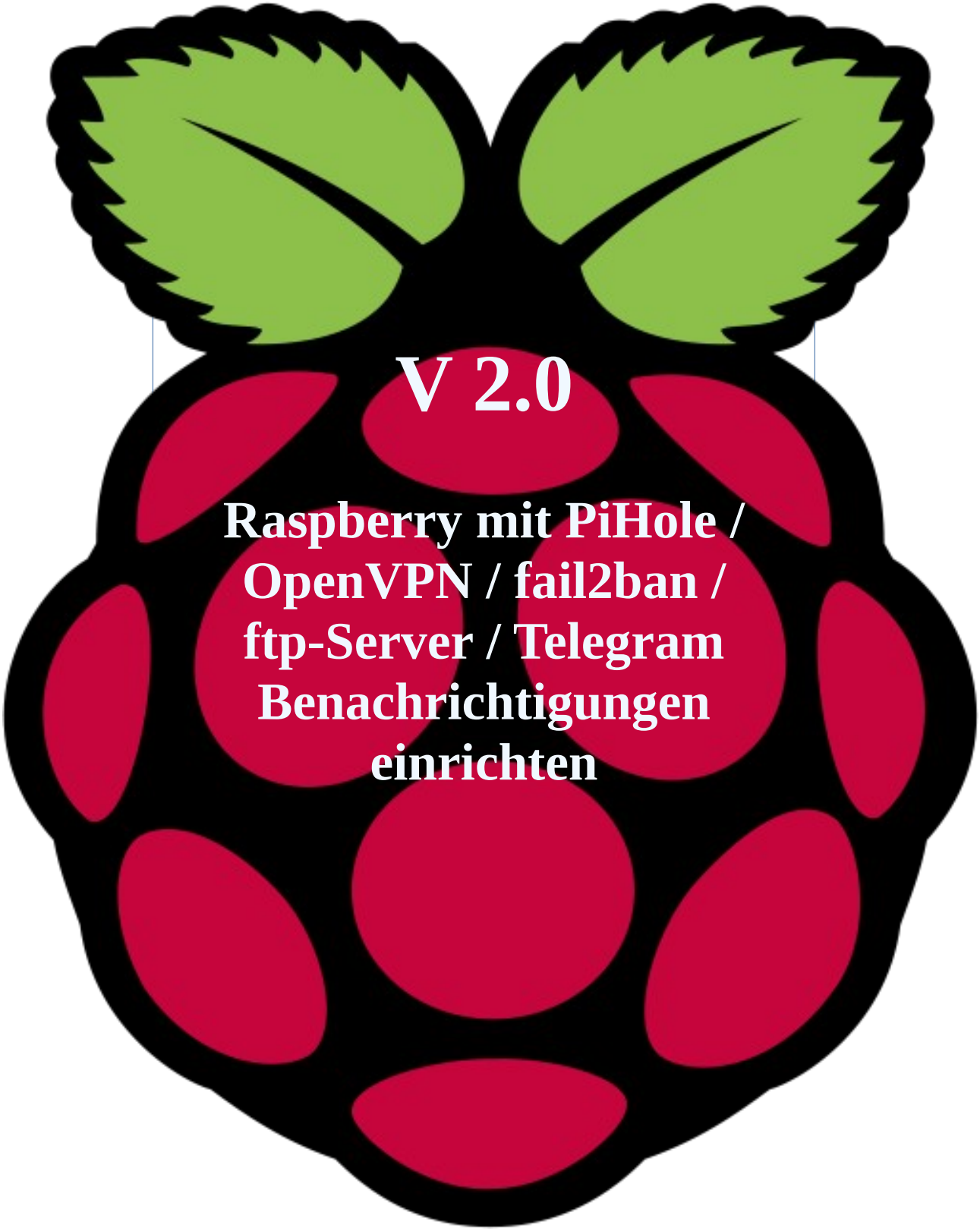

V 2.0

Raspberry mit PiHole / OpenVPN / fail2ban / ftp-Server / Telegram Benachrichtigungen einrichten

1. Raspbian installieren (Datei „SSH“ in der Boot-Partition hinterlegen)
2. Raspbian konfigurieren und updaten
3. «message of the day» löschen
    1. `sudo echo > /etc/motd`
4. Username wechseln
    1. Bei `raspi-config` einstellen dass kein Autologin stattfindet.
    2. Benutzer hinzufügen:
       `sudo adduser username`
    3. Neuer Nutzer als Sudo-Berechtigt eintragen:
       `sudo adduser username sudo`
       Folgendes File löschen:
       `rm /etc/sudoer.d/010_pi-nopasswd`
    4. Als neuer User einloggen
    5. Verzeichnis und Benutzer Pi entfernen:
       `sudo deluser -remove-home pi`
    6. Versionsinfo beim login entfernen
       `touch ~/.hushlogin`
5. PiHole installieren
    1. `curl -sSL https://install.pi-hole.net | bash`
    2. Upstream DNS: Custom (siehe router oder whoer um die aktuellen DNS-Server des ISP einzutragen.
    3. Protokolle auswählen (IPv4 standard. Ggf IPv6 ebenfalls aktivieren falls benötigt)
    4. Als Gateway die Router-IP eintragen
    5. Weblogin-Passwort ändern mit:
       `pihole -a -p`
    6. Im Webinterface: Tools → Create Debug Log → IPv6 Adresse bei erwähntem Fehler anpassen
6. PiVPN installieren
    1. Installation:
       `curl -L https://install.pivpn.io | bash`
    2. Öffnen:
       `sudo nano /etc/dnsmasq.conf`
    3. Hinzufügen:
       `listen-address=127.0.0.1`
       `listen-address=10.8.0.1`
    4. Öffnen: `/etc/openvpn/server.conf`
    5. Hinzufügen bzw abändern:
       `push "dhcp-option DNS 10.8.0.1"`
    6. Abschliessend:
       `service dnsmasq restart`
       `service openvpn restart`
    7. Für Benachrichtigungen bei Verbindungseingang:
       `sudo nano /etc/openvpn/server.conf`
       Am Ende des Files folgendes anfügen:
       `script-security 2`
       `client-connect /path/to/script.sh`
    8. Ggf Zugriffsrechte mit chown entsprechend ändern dass User Nobody zugreifen kann.

7. FTP-Server installieren
    1. apt-get install vsftpd
    2. Folgendes in der Config ggf ändern:
       sudo nano /etc/vsftpd.conf
       anonymous_enable=NO
       local_enable=YES
       write_enable=YES
       local_umask=022
       chroot_local_user=YES
    3. Am Ende des Files noch folgendes einfügen:
       user_sub_token=$USER
       local_root=/home/$USER/ftp
    4. FTP-Ordner erstellen:
       mkdir /home/<USERNAME>/ftp
       mkdir /home/<USERNAME>/ftp/files
    5. Berechtigungen für den Ordner ändern:
       chmod a-w /home/pi/ftp
    6. Server neu starten:
       sudo service vsftpd restart
8. DUC (für noip.com) installieren
    1. Herunterladen und installieren:
       cd /usr/local/src/
       wget http://www.no-ip.com/client/linux/noip-duc-linux.tar.gz
       tar xf noip-duc-linux.tar.gz
       cd noip-2.1.9-1/
       make install
    2. Konfigurieren:
       sudo /usr/local/bin/noip2 -C
    3. Dienst starten:
       sudo /usr/local/bin/noip2
    4. Autostart einrichten:
       sudo cp /usr/local/src/noip-2.1.9-1/debian.noip2.sh /etc/init.d/noip2
       sudo chmod +x /etc/init.d/noip2
       sudo nano /etc/init.d/noip2
    5. Folgendes noch nachtragen:
       ```
       ### BEGIN INIT INFO
       # Provides:          noip2.sh
       # Required-Start:    $remote_fs $local_fs
       # Required-Stop:     $remote_fs $local_fs
       # Should-Start:
       # Should-Stop:
       # Default-Start:     2 3 4 5
       # Default-Stop:      0 1 6
       # Short-Description: Dynamic IP client updater
       # Description:
       ### END INIT INFO
       ```
    6. Befehl ausführen:
       sudo update-rc.d noip2 defaults

9. Fail2Ban installieren

1. Installation:
   `sudo apt-get install fail2ban -y`
2. Konfiguration Ban-Zeit/Gründe
   `sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local`
   `sudo nano /etc/fail2ban/jail.local`
   `ignoreip` eigene IP eintragen
   `bantime` anpassen
   `findtime` anpassen
   `maxretry` anpassen
3. Service neu starten:
   `sudo systemctl restart fail2ban.service`
4. Script bei Ban/Unban ausführen:
   Neue Aktionsdatei erstellen:
   `sudo cp /etc/fail2ban/action.d/dummy.conf /etc/fail2ban/action.d/runscript.conf`
   Datei editieren:
   `sudo nano /etc/fail2ban/action.d/runscript.conf`
   Folgende Optionen belassen, den Rest löschen:
   `actionban = /home/apop85/scripts/f2b_info.sh ban <ip>`
   `actionunban = /home/apop85/scripts/f2b_info.sh unban <ip>`
   Aktion aktivieren:
   `sudo nano /etc/fail2ban/jail.local`
   Bei allen Optionen bei welcher eine Benachrichtigungen erwünscht ist folgendes nachtragen:
   `action = runscript`
   Service neu starten:
   `sudo systemctl restart fail2ban.service`