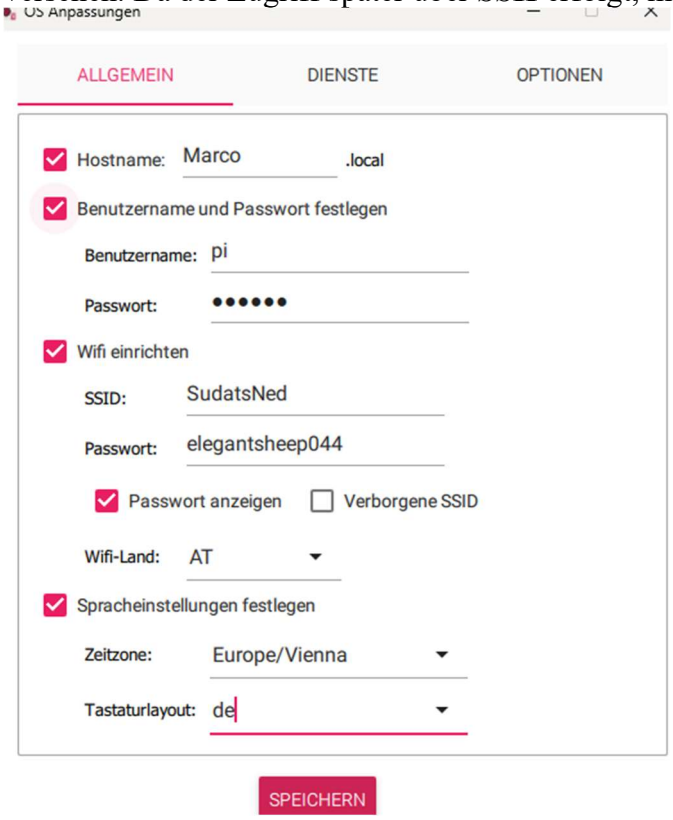
Raspberry Pi und Ntopng – Netzwerküberwachung neu definiert

Ntopng ist mehr als nur ein Überwachungstool.. es ist ein Fenster in die Tiefen des Netzwerks, ein Instrument, das Transparenz schafft, wo sonst Unsichtbarkeit herrscht. Mit einem Raspberry Pi als Basis lässt sich eine leistungsstarke Analyseplattform aufbauen, die Netzwerkaktivitäten in Echtzeit erfasst und interpretiert.

Ein System bereitmachen

Jede Reise beginnt mit einer soliden Grundlage. Der erste Schritt besteht darin, den Raspberry Pi mit dem passenden Betriebssystem auszustatten. **Raspbian OS Bullseye Lite 64Bit** bildet die Basis. Ein Hostname wird gesetzt, der Benutzer `pi` eingerichtet und mit einem Passwort versehen. Da der Zugriff später über **SSH** erfolgt, muss dieser Dienst aktiviert werden.



Sobald die Verbindung steht, beginnt die Vorbereitung:

```
sudo apt-get update
sudo apt-get full-upgrade
sudo reboot
```

Diese Befehle sorgen dafür, dass das System auf dem neuesten Stand ist unerlässlich für einen stabilen Betrieb.

Die Installation von Ntopng

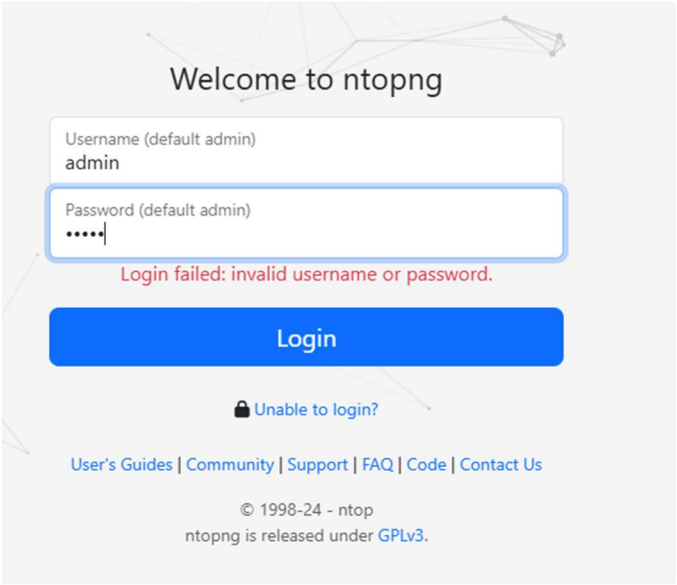
Die eigentliche Magie beginnt mit der Installation von **Ntopng**, einer leistungsfähigen Plattform zur Netzwerküberwachung. Das Paket wird direkt auf den Raspberry Pi geladen und installiert:

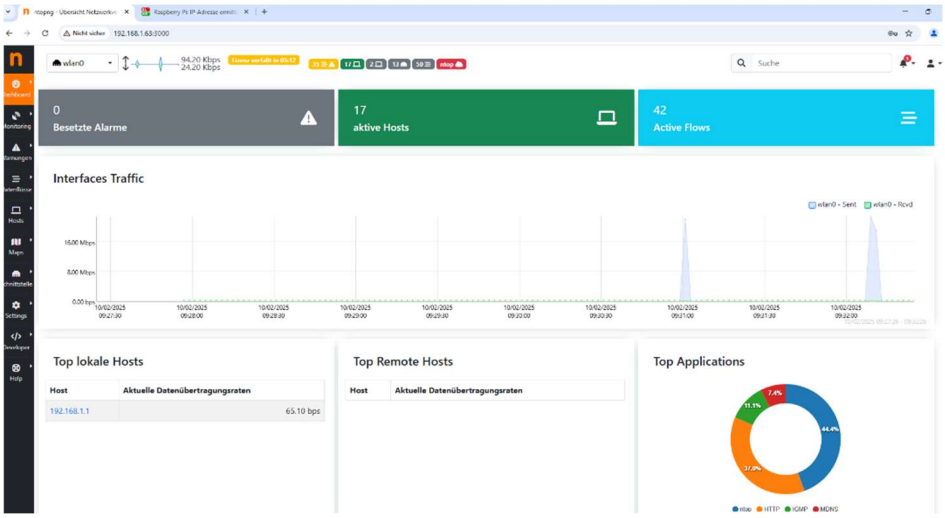
```
wget https://packages.ntop.org/RaspberryPI/apt-ntop.deb
sudo dpkg -i apt-ntop.deb
sudo apt-get update
sudo apt-get install ntopng nprobe
```

Jetzt öffnet sich das Tor zur Analysewelt: Die Weboberfläche von Ntopng wird über den Browser aufgerufen: `http://192.168.1.63:3000`

Zum ersten Mal eingeloggt mit:

- **Benutzer:** `admin`
- **Passwort:** `admin`





Netzwerk stabilisieren – Die IP-Adresse festlegen

Damit der Raspberry Pi immer unter der gleichen Adresse erreichbar ist, kann eine statische IP eingerichtet werden. Dafür öffnet sich die Konfigurationsdatei:

```
sudo nano /etc/dhcpcd.conf
```

Die Anpassungen erfolgen in den folgenden Zeilen:

```
interface eth0
static ip_address=192.168.1.63/24
static routers=192.xxx.xxx.x
static domain_name_servers=192.xxx.xxx.x
```

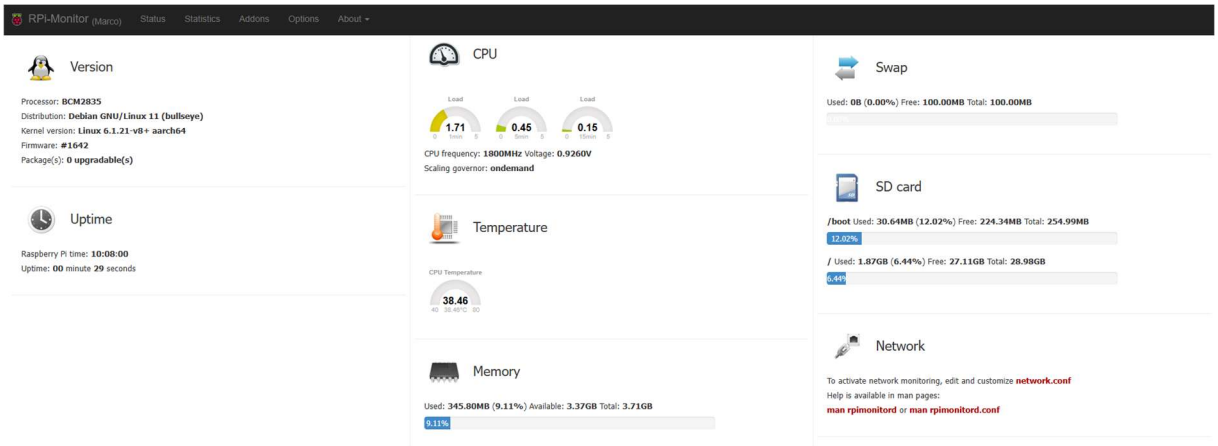
Jede Netzwerkkonfiguration ist einzigartig… die Werte sollten entsprechend angepasst werden.

Speichern mit `Strg + O`, verlassen mit `Strg + X`. Ein Neustart setzt die Änderungen in Kraft:

```
sudo reboot
```

Die Kontrolle über die Hardware behalten

Wer über das Netzwerk wacht, sollte auch seinen Raspberry Pi im Blick behalten. Hier kommt **RPi Monitor** ins Spiel:




```
sudo wget http://goo.gl/vewCLL -O /etc/apt/sources.list.d/rpimonitor.list
sudo apt-key adv --recv-keys --keyserver keyserver.ubuntu.com 2C0D3C0F
sudo apt-get update
sudo apt-get install rpimonitor
```

Ein Update sichert die neuesten Informationen:

```
sudo /etc/init.d/rpimonitor update
sudo reboot
```

Nun sind die Systemdaten jederzeit abrufbar unter: `http://192.168.1.63:8888/`

Die Möglichkeiten von Ntopng entdecken

Mit der Installation allein ist es nicht getan. **Ntopng** öffnet ein Fenster in das Netzwerkgeschehen:

- **Echtzeit-Überwachung des Datenverkehrs**
- **Detaillierte Analyse von Hosts, Protokollen und Anwendungen**
- **Erkennung von ungewöhnlichen oder gefährlichen Netzwerkaktivitäten**
- **Visualisierung der Bandbreitennutzung**
- **Möglichkeiten zur Integration mit externen Tools wie Grafana oder ELK-Stack**
- **Erweiterbar durch nProbe für noch tiefere Analysen**