# sudo raspi-config

* update
* Change the Pi password
* Disable "Boot to Desktop"
* Update your Locale settings
* Set your Hostname to curingpi
* Set the Memory Split 16
* Ensure SSH is enabled
* sudo reboot

# configure wlan

* sudo nano /etc/wpa\_supplicant/wpa\_supplicant.conf
* enter
  + network={  
            ssid="The\_SSID"  
               psk="Your\_wifi\_password"      
        }
* sudo nano /etc/network/interfaces
* change *iface wlan0 inet \** to *iface wlan0 inet static*
* add below
  + *address 192.168.x.x*
  + *netmask 255.255.255.0*
  + *network 192.168.x.x*
  + *broadcast 192.168.x.255*
  + *gateway 192.168.x.x*
* Remove any existing leases
* sudo rm /var/lib/dhcp/\*
* sudo reboot

# create new user

* groups
* sudo useradd -m -G adm,dialout,cdrom,sudo,audio,video,plugdev,games,users,input,netdev,gpio,i2c,spi USERNAME  
  change line according to your groups
* sudo passwd USERNAME

# delete pi user

* change to created user
* sudo deluser --remove-all-files pi

# disable root login from ssh

* sudo nano /etc/ssh/sshd\_config
* PermitRootLogin no

# rpi aktualisieren

* apt-get update
* apt-get upgrade

# create firewall with iptables

[**https://www.linode.com/docs/security/securing-your-server#basic-iptables-rulesets-for-ipv4-and-ipv6**](https://www.linode.com/docs/security/securing-your-server#basic-iptables-rulesets-for-ipv4-and-ipv6)

* sudo nano /tmp/v4
  + \*filter  
      
    # Allow all loopback (lo0) traffic and reject traffic  
    # to localhost that does not originate from lo0.  
    -A INPUT -i lo -j ACCEPT  
    -A INPUT ! -i lo -s 127.0.0.0/8 -j REJECT  
      
    # Allow ping and traceroute.  
    -A INPUT -p icmp --icmp-type 3 -j ACCEPT  
    -A INPUT -p icmp --icmp-type 8 -j ACCEPT  
    -A INPUT -p icmp --icmp-type 11 -j ACCEPT  
      
    # Allow SSH connections.  
    -A INPUT -p tcp -m state --state NEW --dport 22 -j ACCEPT  
      
    # Allow HTTP and HTTPS connections from anywhere  
    # (the normal ports for web servers).  
    -A INPUT -p tcp --dport 80 -j ACCEPT  
    -A INPUT -p tcp --dport 443 -j ACCEPT  
      
    # Accept inbound traffic from established connections.  
    -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT  
      
    # Log what was incoming but denied (optional but useful).  
    -A INPUT -m limit --limit 5/min -j LOG --log-prefix "iptables\_INPUT\_denied: " --log-level 7  
      
    # Reject all other inbound.  
    -A INPUT -j REJECT  
      
    # Log any traffic which was sent to you  
    # for forwarding (optional but useful).  
    -A FORWARD -m limit --limit 5/min -j LOG --log-prefix "iptables\_FORWARD\_denied: " --log-level 7  
      
    # Reject all traffic forwarding.  
    -A FORWARD -j REJECT  
      
    COMMIT
* sudo nano /tmp/v6
  + \*filter  
      
    # Allow all loopback (lo0) traffic and reject traffic  
    # to localhost that does not originate from lo0.  
    -A INPUT -i lo -j ACCEPT  
    -A INPUT ! -i lo -s ::1/128 -j REJECT  
      
    # Allow ICMP  
    -A INPUT  -p icmpv6 -j ACCEPT  
      
    # Allow HTTP and HTTPS connections from anywhere  
    # (the normal ports for web servers).  
    -A INPUT -p tcp --dport 80 -j ACCEPT  
    -A INPUT -p tcp --dport 443 -j ACCEPT  
      
    # Accept inbound traffic from established connections.  
    -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT  
      
    # Log what was incoming but denied (optional but useful).  
    -A INPUT -m limit --limit 5/min -j LOG --log-prefix "ip6tables\_INPUT\_denied: " --log-level 7  
      
    # Reject all other inbound.  
    -A INPUT -j REJECT  
      
    # Log any traffic which was sent to you  
    # for forwarding (optional but useful).  
    -A FORWARD -m limit --limit 5/min -j LOG --log-prefix "ip6tables\_FORWARD\_denied: " --log-level 7  
      
    # Reject all traffic forwarding.  
    -A FORWARD -j REJECT  
      
    COMMIT
* now:
* sudo iptables-restore < /tmp/v4  
  sudo ip6tables-restore < /tmp/v6
* sudo apt-get install iptables-persistent
  + - answer yes to save current rules

# installing fail2ban

* sudo apt-get install fail2ban
* sudo nano /etc/fail2ban/jail.conf
* change settings accordingly
* sudo reboot //oder fail2ban service neustarten

# change ssh port

* sudo nano /etc/ssh/sshd\_config
* change port 22 to port YOURPORT
* sudo service ssh restart

# Change IPtable rule

* sudo nano /etc/iptables/rules.v4
* change port 22 to YOURPORT

# send email on ssh login

* sudo apt-get install sendemail
* sudo nano /etc/ssh/sshrc
* ip=`echo $SSH\_CONNECTION | cut -d " " -f 1`  
    
  logger -t ssh-wrapper $USER login from $ip  
  echo "User $USER just logged in from $ip" | sendemail -q -u "SSH Login Warning" -f "SSH Login Script <YOURFROM@web.de>" -s smtp.web.de:25 -xu YOURSMTOLOGINNAME -xp YOURPW  -t "YOURNAME <YOURTOEMAIL@gmail.com>" -o tls=yes$

# DynDnsclient installieren

[**http://www.forum-raspberrypi.de/Thread-tutorial-dynamic-dns**](http://www.forum-raspberrypi.de/Thread-tutorial-dynamic-dns)

* apt-get install ddclient
* sudo nano /etc/ddclient.conf
* ssl=yes
* protocol=dyndns2
* use=web, web=checkip.dyndns.org/
* server=dyndns.strato.com/nic/update
* login=USERHERE
* password='YOURDNSPWHERE'
* HOSTHERE
* check if settings work
* sudo ddclient -daemon=0 -debug -verbose -noquiet 2 /etc/ddclient.conf
* service neustarten
* sudo /etc/init.d/ddclient restart

# git core essentials installieren

* sudo apt-get install git-core

# Mongodb installieren

* git clone <https://github.com/svvitale/mongo4pi/>
* cd mongo4pi
* sudo ./install.sh
* automatisch gestartet sonst
* sudo /etc/init.d/mongod start
* zum stoppen
* sudo /etc/init.d/mongod stop
* execute mongo shell from
* /opt/mongo/bin/mongo