Linux

- Allgemein
  - Zugriffsrechte fÃ¼r Dateien und Ordner
  - Debian Spiegel-Server Ã¤ndern
- Fun
  - Asciiquarium installieren
- Server Installation
  - LAMP Installation (MySQL, Apache, PHP)
  - Pi-hole installieren
  - Samba Netzwerkfreigabe erstellen
  - Linux automatisch aktualisieren
  - HTTPS Reverse Proxy mit Nginx konfigurieren
  - Nginx Reverse Proxy - WebSocket verliert die Verbindung
  - Apache2 SSL Virtualhost SSL Konfiguration
- Service Konfiguration
  - E-Mail bei Linux Updates
  - E-Mail Benachrichtigung bei SSH Login
  - Port von sendmail Ã¤ndern
  - SSH Root Login verbieten
  - Apache - Error 404 "Objekt nicht gefunden"
- Terminal Befehle
  - Arbeitsspeicher im Cache freigeben
  - Linux Version anzeigen lassen

    - Mit sendmail Mails verschicken
    - Skript ausfÃ¼hrbar machen
    - Belegte Ports in Linux ausgeben
    - CPU Informationen und Auslastung im Terminal anzeigen
    - Hostnamen des Rechners / Servers Ã¤ndern
    - DNS auf Linux Rechner deaktivieren
    - Mit MariaDB-Client auf einen anderen SQL-Server verbinden
    - Verzeichnis und Dateien in ein ZIP-Archiv verschieben
    - Partition von Debian im laufenden Betrieb vergrÃ¶ÃŸern

- GRUB Bootloader
    - Standard Boot Partition Ã¤ndern
    - Bootloader Hintergrund Ã¤ndern

- Problembeseitigung
    - Debian Fehlermeldung: dpkg: warning: 'ldconfig' not found in PATH or not executable.

- Wireguard
    - Wireguard Client auf Debian installieren

Allgemein

Allgemein

Zugriffsrechte fÃ¼r Dateien und Ordner

Einleitung

In Linux herrscht ein striktes Berechtigungssystem. Wir kÃ¶nnen fÃ¼r jeden Ordner festlegen, wer welche Datei schreiben, lesen oder ausfÃ¼hren darf. Diese Konfiguration machen wir Ã¼ber das Terminal. Ansonsten kÃ¶nnen wir die Berechtigungen auch Ã¼ber die GUI setzen.

Zur Verwaltung der Berechtigungen verwenden wir den Befehl **chmod**. Mit diesen kÃ¶nnen wir Berechtigungen festlegen, verÃ¤ndern oder ganz entfernen.

Syntax von chmod

Wenn wir den Befehl **chmod** verwenden mÃ¶chten, mÃ¼ssen wir erstmal die Syntax des Befehls nachvollziehen.

```
chmod [optionen] <maske> <datei>
```

Unter **maske** verstehen wir die Berechtigungsmaske. Die Zuteilung kann Symbolisch oder Numerisch umgesetzt werden.

Symbolische Zuteilung

Wenn wir die Berechtigungen Ã¼ber Symbole und Buchstaben Ã¤ndern mÃ¶chten, wird die Maske in 3 Teilbereiche aufgeteilt.

- Benutzerkategorie
- Operator
- Rechte

Die Rechte werden von der Benutzerkategorie immer durch einen Operator getrennt. Der Operator gibt an, ob die Rechte jeweils hinzugefÃ¼gt, entfernt oder gesetzt werden.

Benutzerkategorie	
u	Besitzer
g	Gruppe
o	Andere
a	All (Besitzer, Gruppe, Andere)

Operator	
+	Rechte hinzufügen
-	Rechte entfernen
=	Rechte neu setzen

Rechte	
r	Lesen
w	Schreiben
x	Auführen

Syntax Beispiele:

```
chmod a+rwx datei.txt

chmod +x script.sh

chmod u=rw,g=rw,o=r datei.txt
```

Numerische Zuteilung

Im Gegenteil zu der Symbolischen Zuordnung, kÃ¶nnen Berechtigungen auch Ã¼ber die Numerische Zuteilung gesetzt werden. Dort wird eine dreistelle Zahl angegeben. Diese teilt mit, welche Berechtigungen, welche Ebene bekommt.

- **1. Zahl** = Besitzer
- **2. Zahl** = Gruppe
- **3. Zahl** = Andere

Die Rechte werden dann mit einer Nummer identifiziert. Die Zahl **751** gibt z.B. die Berechtigung fÃ¼r den Besitzer **Vollzugriff**, fÃ¼r die Gruppe **Lesen, AusfÃ¼hren** und fÃ¼r andere auf **Nur AusfÃ¼hren**.

Berechtigungen	
7	Vollzugriff
6	Lesen, Schreiben
5	Lesen, Ausführen
4	Nur Lesen
3	Schreiben, Ausführen
2	Nur Schreiben
1	Nur Ausführen
0	Keine Berechtigungen

Syntaxbeispiele:

```
chmod 777 datei.txt


chmod -R 700 /footer/topbar
```

Optionen

Um den Befehl jetzt noch intelligenter zu gestalten, gibt es die **Optionen**. Mit den Optionen kÃ¶nnen wir dem Befehl noch etwas mitgeben wie er sich verhalten soll. Die Option geben wir mit einem **Bindestrich** vorne dran an, und wir schreiben dann die entsprechenden Buchstaben dahinter.

Optionen	
-c	hat die gleiche Funktion wie -**v**, gibt aber nur Rückmeldung wenn etwas geändert wird.
-f	Unterdrückt Fehlermeldungen
-R	Damit werden die Berechtigungen Rekursiv auf Unterverzeichnisse und Unterdateien geschrieben.
-v	Zeigt alles an was der Befehl gerade am System macht.

Allgemein

Debian Spiegel-Server Ã¤ndern

Einleitung

In diesem Beitrag erklÃ¤re ich kurz, wie wir schnell unter Debian den Spiegelserver auf einen anderen Spiegelserver Ã¤ndern kÃ¶nnen. Dazu geben wir noch einen Parameter mit, mit dem sich das Programm automatisch den besten Spiegelserver automatisch heraussucht.

Spiegelserver Ã¤ndern

Um den Spiegelserver zu Ã¤ndern, mÃ¼ssen wir im ersten Schritt das Programm installieren. Dazu benÃ¶tigen wir erstmal die Python Paket Installer PIP.

```
sudo apt install pip -y
```

Im Anschluss installieren wir das benÃ¶tigte, Programm, um schnell den Spiegelserver zu Ã¤ndern.

```
sudo pip3 install apt-mirror-updater
```

Spiegelserver schnell Ã¤ndern (Automatische Suche)

Damit das Programm den Spiegelserver selbst heraussucht, geben wir den Parameter -b mit. Dann liest das Programm die Spiegelserver selbst ein, und probiert alle durch. Den besten installiert er fÃ¼r sich selbst.

```
sudo apt-mirror-updater -b
sudo apt-mirror-updater --find-best-mirror


sudo apt-mirror-updater -a
sudo apt-mirror-updater --auto-change-mirror
```

MÃ¶gliche Spiegelserver anzeigen

Um die mÃ¶glichen Spiegelserver anzuzeigen, verwenden wir den Parameter -L. Dann liest das Programm die Spiegelserver-Listen ein, und zeigt uns die mÃ¶glichen Spiegelserver.

```
sudo apt-mirror-updater -c=<URL>
sudo apt-mirror-updater --change-mirror=<URL>
```

Fun

Fun

Asciiquarium installieren

Einleitung

Mit Asciiquarium haben wir unser eigenes Aquarium in unserem Terminal. Dieses Projekt hat keinen sinnhaften Grund, aber ist ganz witzig es sich mal anzuschauen. Es sollte daher nicht in Produktiv System verwendet werden, da dort auf eine Minimale Installation gesetzt werden sollte um wenig bis keine Einfalltore zu haben.

Installation

Zuerst mÃ¼ssen wir uns mit dem Terminal unseres Linux Server / Clients verbinden. Wir melden uns dort als *root* an damit wir nachher die Befehle ohne **sudo** absetzen kÃ¶nnen.

Im ersten Abschnitt mÃ¼ssen wir **Term-Animation** installieren. Dazu mÃ¼ssen wir ein paar Befehle absetzen. Zuerst installieren wir das Paket **X**.

```
apt install libcurses-perl -y
```

Dann navigieren wir in das Verzeichnis **/tmp**, laden die benÃ¶tigten Dateien herunter und entpacken diese. Im Anschluss navigieren wir in das Verzeichnis.

```
cd /tmp
wget http://search.cpan.org/CPAN/authors/id/K/KB/KBAUCOM/Term-Animation-2.6.tar.gz
tar -zxvf Term-Animation-2.6.tar.gz
cd Term-Animation-2.6
```

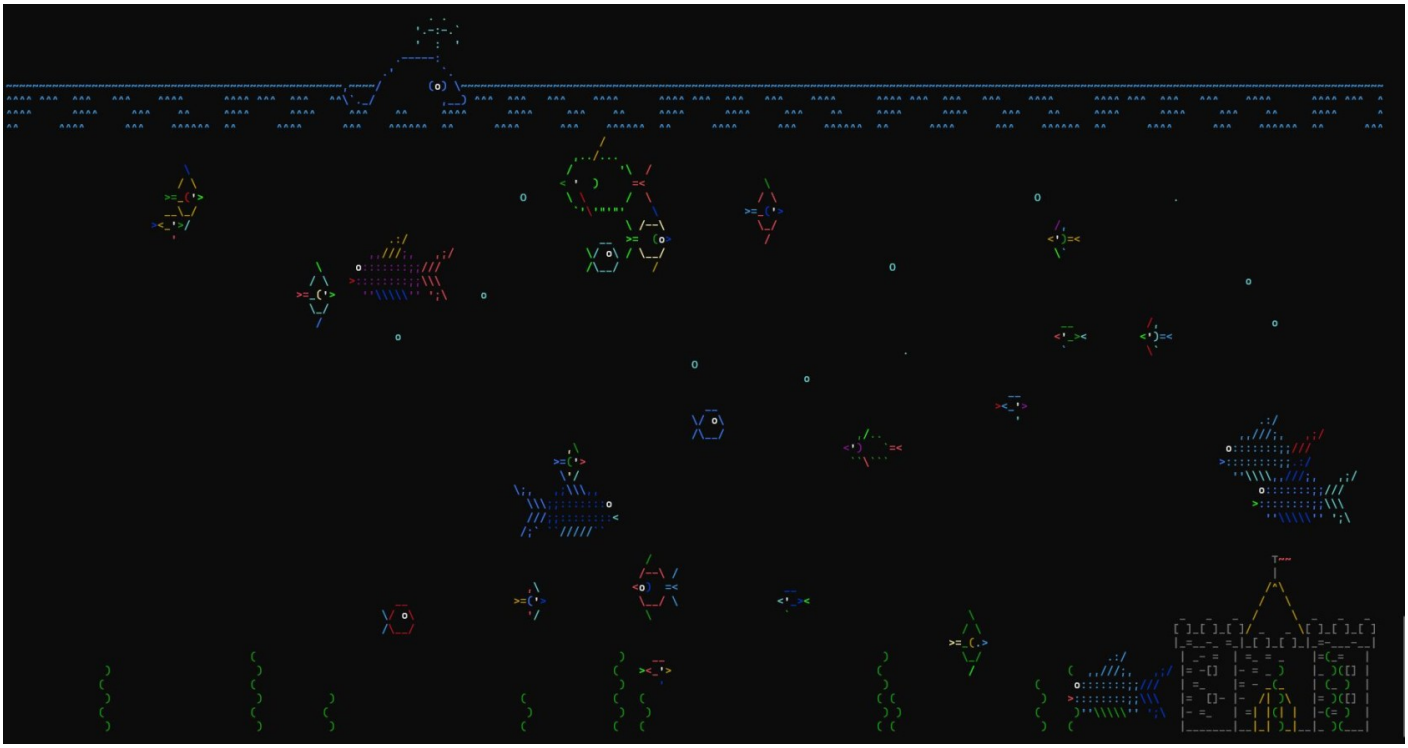
Als nÃ¤chsten Schritt fÃ¼hren wir das **Makefile Perl Skript** aus und schlieÃŸen dann im Abschluss die Installation ab.

```
perl Makefile.PL && make && make test
make install
```

Jetzt kÃ¼mmern wir uns darum das wir **Asciiquarium** installieren. Dazu wechseln wir wieder in das **/tmp** Verzeichnis und laden das Perl Skript herunter und entpacken dieses wieder, kopieren es in das **/usr/local/bin** Verzeichnis und passen die Berechtigungen an, damit das Skript ausfÃ¼hrbar ist.

```
cd /tmp
wget --no-check-certificate http://www.robobunny.com/projects/asciiquarium/asciiquarium.tar.gz
tar -zxvf asciiquarium.tar.gz
cp asciiquarium /usr/local/bin/
chmod 0755 /usr/local/bin/asciiquarium
```

Wenn wir jetzt unser Aquarium begutachten wollen, starten wir es mit dem Befehl **asciiquarium**.



Server Installation

LAMP Installation (MySQL, Apache, PHP)

Einleitung

In dieser Anleitung beschreibe ich kurz wie wir einen **LAMP Webserver** installieren.
Ein **LAMP Webserver** ist eine Installationskombination von **Apache, MySQL / MariaDB** und **PHP** .

Voraussetzungen

Um diese Installation durchfÃ¼hren zu kÃ¶nnen sind folgende Voraussetzungen gegeben:

- Zugriff auf die Konsole Ã¼ber SSH / Telnet / Lokal
- Root Rechte / sudo Rechte
- Debian 11
- Internet Anbindung des Servers

Apache Webserver Installation

Um den Apache Webserver zu installieren, aktualisierst du zuerst die Paketquellen und installierst ggf. Updates und entfernst nicht mehr benÃ¶tigte Pakete.

```
sudo apt-get update && apt-get upgrade -y && apt-get autoremove -y
```

Als nÃ¤chstes installierst du den Apache2 Webserver.

```
sudo apt install apache2 -y
```

Du kannst jetzt die Installation mit dem Befehl Ã¼berprÃ¼fen.

> Wenn du eine UFW Firewall mit installiert und aktiviert hast, musst du die Ports auf der Firewall freigeben!

```
sudo ufw allow 80/tcp && \
sudo ufw allow 443/tcp && \
sudo ufw reload
```

MariaDB Datenbank Installation

Um jetzt die MariaDB Datenbank zu installieren aktualisierst du zuerst wieder die Paket Quellen, installierst Updates und entfernst nicht mehr benÃ¶tigte Pakete.

```
sudo apt-get update && apt-get upgrade -y && apt-get autoremove -y
```

Als nÃ¤chstes installierst du jetzt die MariaDB Datenbank.

```
sudo apt install mariadb-server -y
```

Und jetzt fÃ¼hren wir ein Skript aus. Dieses lÃ¤sst uns Sicherheitseinstellungen fÃ¼r unseren Datenbank Server einstellen. Dieses Ã¶ffnen wir mit folgendem Befehl

```
mysql_secure_installation
```

Hier werden einige Dinge abgefragt. Diese Einstellungen werden wir jetzt gemeinsam setzen.

- Zuerst Enter drÃ¼cken (Wir haben bisher kein root Kennwort gesetzt fÃ¼r den Datenbank Benutzer)
- Debian 11: Die Unix Authentifizierung lehnen wir mit **n** ab.
- Jetzt **Y** eingeben. Wir setzen nun ein Kennwort fÃ¼r den **Root** Datenbank Benutzer.
- Als nÃ¤chstes **Y** eingeben. Wir wollen alle unbekannten Benutzer lÃ¶schen.
- Dann geben wir wieder **Y** ein. Wir unterbinden damit eine Anmeldung des **Root Benutzers** auÃŸerhalb unseres Servers.
- Und wieder geben wir **Y** ein. Damit wird die Test Datenbank und die Rechte dorthin gelÃ¶scht.
- Als letztes geben wir wieder ein **Y** ein. Damit werden die Berechtigungen einmal neu geladen.

Nun kannst du dich mit folgendem Befehl auf dem SQL Server einloggen. Du wirst nach der Eingabe nach dem Kennwort des Root Benutzers gefragt. Sobald du dieses eingegeben hast, kannst du SQL Befehle absetzen.

```
mysql -u root -p
```

> Wenn kein Passwort fÃ¼r Root angegeben wurde, loggt sich der Benutzer automatisch auf dem Server ein.

Installation von PHP 7.4

Um unsere Installation abzuschlieÃŸen, installieren wir jetzt PHP7.4

PHP ist eine Serverseitige Programmiersprache. Damit kÃ¶nnen Befehle direkt auf dem Server ausgefÃ¼hrt werden, z.B. werden Datenbank Abfragen hÃ¤ufig Ã¼ber PHP durchgefÃ¼hrt.

```
sudo apt install php7.4 php7.4-cli php7.4-common php7.4-curl php7.4-gd php7.4-intl php7.4-json php7.4-mbstring php7.4-mysql php7.4-opcache php7.4-readline php7.4-xml php7.4-xsl php7.4-zip php7.4-bz2 libapache2-mod-php7.4 -y
```

Du hast jetzt erfolgreich PHP 7.4 mit Modulen installiert!

Installation von PHP 8.0

Um unsere Installation abzuschlieÃŸen, installieren wir jetzt PHP7.4

PHP ist eine Serverseitige Programmiersprache. Damit kÃ¶nnen Befehle direkt auf dem Server ausgefÃ¼hrt werden, z.B. werden Datenbank Abfragen hÃ¤ufig Ã¼ber PHP durchgefÃ¼hrt.

```
sudo apt install php8.0 php8.0-cli php8.0-common php8.0-curl php8.0-gd php8.0-intl php8.0-mbstring php8.0-mysql php8.0-opcache php8.0-readline php8.0-xml php8.0-xsl php8.0-zip php8.0-bz2 libapache2-mod-php8.0 -y
```

Du hast jetzt erfolgreich PHP 8.0 mit Modulen installiert!

Optional: Installation von phpMyAdmin

Du kannst Optional auch phpMyAdmin installieren um deine Datenbank Ã¼ber eine WeboberflÃ¤che zu verwalten.

Als erstes wechselst du in das Verzeichnis in dem du phpMyAdmin ablegen mÃ¶chtest.

```
cd /var/www
```

Nun lÃ¤dst du das Verpackte Archiv mit den Dateien fÃ¼r phpMyAdmin herunter.

```
wget https://www.phpmyadmin.net/downloads/phpMyAdmin-latest-all-languages.zip -O phpmyadmin.zip
```

Als nÃ¤chstes entpackst du das ZIP Archiv und lÃ¶schst das alte Verzeichnis.

```
sudo unzip phpmyadmin.zip && sudo rm phpmyadmin.zip
```

Nun verÃ¤nderst du den Namen des Ordners in phpMyAdmin.

```
mv phpMyAdmin-*-all-languages phpmyadmin
```

Jetzt verÃ¤nderst du die Berechtigungen auf das Verzeichnis.

```
sudo chmod -R 0755 phpmyadmin
```

Und damit wir dann Ã¼ber den Web Browser auf phpMyAdmin zugreifen kÃ¶nnen, erstellen wir eine Konfigurationsdatei fÃ¼r den Apache2 Webserver.

```
sudo nano /etc/apache2/conf-available/phpmyadmin.conf
```

Dort fÃ¼gst du folgende Konfiguration ein.

```
Alias /phpmyadmin /var/www/phpmyadmin

<Directory /var/www/phpmyadmin>
    Options SymLinksIfOwnerMatch
    DirectoryIndex index.php
</Directory>

<Directory /var/www/phpmyadmin/templates>
    Require all denied
</Directory>
<Directory /var/www/phpmyadmin/libraries>
    Require all denied
</Directory>
<Directory /var/www/phpmyadmin/setup/lib>
    Require all denied
</Directory>
```

Sobald du mit der Tastenkombination **STRG + X** und danach **Y** die Datei gespeichert hast, aktivieren wir jetzt die Konfigurationsdatei.

```
sudo a2enconf phpmyadmin && sudo systemctl reload apache2
```

Um die Installation abzuschlieÃŸen, erstellen wir temporÃ¤res Verzeichnis im **phpMyAdmin Verzeichnis** und vergeben fÃ¼r dieses die entsprechende Berechtigung.

```
sudo mkdir /var/www/phpmyadmin/tmp/ && sudo chown -R www-data:www-data /var/www/phpmyadmin/tmp/
```

Du kannst dich nun mit den entsprechenden Datenbank Benutzern anmelden. Wenn sich **phpMyAdmin** auf dem selben Server wie die Datenbank befindet, musst du keinen Server angeben und du kannst dich mit einem Benutzer anmelden mit dem Host **localhost**. Kannst dich also auch als **root** anmelden.

Pi-hole installieren

Einleitung

Pi-hole ist ein kleiner Ad Blocker der als DNS Server arbeitet. Alle Anfragen die Ã¼blicherweise an einen Google DNS / Cloudflare DNS getÃ¤tigt werden, werden Ã¼ber das Pi-hole gesteuert. Dieser filtert die Antworten von Google und Co. nach EintrÃ¤gen die als Werbung markiert sind. So ist es mÃ¶glich das du im gesamten Netzwerk weniger bis keine Werbung mehr hast.

Installation

Es gibt 4 Wege Pi-hole zu installieren, alle werden hier beschrieben. Du musst dem Pi-hole eine **Statische IP-Adresse** geben damit dieser arbeiten kann. Du trÃ¤gst spÃ¤ter beim DHCP Server die IP-Adresse des Pi-hole's an. Wenn sich ein Client eine IP-Adresse zieht, erhÃ¤lt er zugleich die IP-Adresse des DNS Servers und alle Anfragen werden dann Ã¼ber das Pi-hole gesteuert.

Automatische Installation

Wenn du Pi-hole sich automatisch installieren lassen mÃ¶chtest, musst du nur den unten stehenden Befehl verwenden.

```
curl -sSL https://install.pi-hole.net | bash
```

Es wird hier der eigentliche Pi-hole Dienst installiert sowie ein leichtgewichtiger **lighttpd** Webserver installiert. Bei der Installation wirst du unter anderem auch gefragt ob ein Web Server erwÃ¼nscht ist.

Am Ende der Installation wird dir das Administrator Kennwort angezeigt, mit diesem meldest du dich im Web Interface an um Konfigurationen vorzunehmen.

Repository klonen und Skript ausfÃ¼hren

Als zweiten Weg kannst du das Repository von Github klonen und das entsprechende Installationsskript ausfÃ¼hren.

```
git clone --depth 1 https://github.com/pi-hole/pi-hole.git Pi-hole
cd "Pi-hole/automated install/"
sudo bash basic-install.sh
```

Installer herunterladen und ausfÃ¼hren

Wahlweise kannst du auch den dritten Weg wÃ¤hlen und den Installer herunterladen und ausfÃ¼hren um den Installationsprozess zu starten.

```
wget -O basic-install.sh https://install.pi-hole.net
sudo bash basic-install.sh
```

Installation Ã¼ber Docker

Als letzte MÃ¶glichkeit kannst du auch zu einer Installation Ã¼ber Docker tendieren. Die **docker-compose.yml** Datei findest du unten stehend.

```
version: "3"

services:
  pihole:
    container_name: server_pihole
    image: pihole/pihole:latest
    ports:
      - "53:53/tcp"
      - "53:53/udp"
      - "67:67/udp"
      - "80:80/tcp"
    environment:
      TZ: 'Europe/Berlin'
      WEBPASSWORD: 'Pa$$w0rd'
    volumes:
      - './etc-pihole:/etc/pihole'
      - './etc-dnsmasq.d:/etc/dnsmasq.d'
    cap_add:
      - NET_ADMIN
    restart: unless-stopped
```

Pi-hole CLI Befehle

Pi-hole Befehle	
Verwendung	**Befehl**
Grundbefehl	pihole
Gravity aktualsieren	pihole updateGravity
Pi-hole aktualisieren	pihole updatePihole
Pi-hole Status einsehen	pihole status
Pi-hole Version einsehen	pihole version
Administrator Kennwort ändern	pihole -a -p

Samba Netzwerkfreigabe erstellen

Einleitung

Du kannst mit Samba einen Server erstellen, auf dem du deine Dokumente in einem Netzwerkfreigabe Ordner ablegen kannst. Diesen kannst du dann unter Linux, Windows, Mac OS integrieren und so von jedem GerÃ¤t Netzwerkweit auf deine Dokumente zugreifen.

> **Achtung:** Samba 1.0 zÃ¤hlt als veraltet und sollte daher nur in lokalen abgesicherten Netzwerken installiert werden.

Installation

Um die Installation durchfÃ¼hren zu kÃ¶nnen, gibt es folgende Voraussetzungen:

- Debian 10 / 11
- root oder sudo Rechte
- Konsolenzugriff per SSH / Telnet / Lokal
- Internetanbindung des Servers

Zuerst installieren wir das Paket **samba**

```
sudo apt-get install samba
```

Als zweiten Schritt sichern wir die derzeitige Samba Konfiguration. Dieses Backup dient zum eventuellen ZurÃ¼ckspielen auf den Ursprungszustand.

```
sudo mv /etc/samba/smb.conf /etc/samba/smb.backup
```

Und nun konfigurieren wir den Samba Server. Du erstellst und Ã¶ffnest die neue Konfigurationsdatei im nÃ¤chsten Schritt.

```
sudo nano /etc/samba/smb.conf
```

Dort fÃ¼gst du die Konfiguration ein und speicherst die Datei mit der Tastenkombination `STRG + X` und danach `Y` .

```
[global]
workgroup = smb
security = user
map to guest = Bad Password

[homes]
comment = Home Directories
browsable = no
read only = no
create mode = 0750

[share]
path = /var/share/
public = yes
writable = yes
comment = smb share
printable = no
guest ok = yes
```

In der Konfigurationsdatei kannst du dann noch den Pfad zur Dateiablage verÃ¤ndern oder auch den Namen der Freigabe von **share** auf einen anderen beliebigen setzen.

> **Info:** Du verbindest das Netzlaufwerk dann Ã¼ber den UNC Namen mit dem Freigabe Namen dahinter.
> **Beispiel:** \\192.168.1.13\share

Um dann Daten abzulegen muss der Ordner ggf. erst erstellt werden und dann mit Schreibe und Lese Berechtigungen fÃ¼r Public versehen werden.

Die Berechtigungen fÃ¼r die Benutzer werden dann Ã¼ber die Samba Freigabe gesteuert.

```
sudo mkdir /var/share sudo chmod -R 777 /var/share
```

Und als letztes starten wir den Samba Service neu. Samba liest dann die neue Konfigurationsdatei ein, und die Freigabe ist dann erreichbar.

```
sudo systemctl restart smbd.service
```

Du kannst den Status des Samba Service auch Ã¼berprÃ¼fen. Setze dazu den folgenden Befehl ab:

```
sudo systemctl status smbd.service
```

Linux automatisch aktualisieren

Einleitung

In diesem Beitrag gehe ich drauf ein, wie wir mithilfe des Paketes **cron-apt** unseren Debian Server automatisch aktualisieren. Damit kÃ¶nnen wir sicherstellen, dass wenn wir im Urlaub oder nicht anwesend sind, unser Server immer auf dem aktuellen Stand ist.

Installation des Paketes

Dazu mÃ¼ssen wir zuerst die **Paketquellen aktualisieren** und gegebenenfalls **Updates installieren**, wenn diese vorhanden sind.

```
sudo apt update && sudo apt upgrade -y
```

Im nÃ¤chsten Schritt installieren wir jetzt das Paket **cron-apt**.

Dazu geben wir folgenden Befehl in die Konsole ein.

```
sudo apt install cron-apt -y
```

Konfiguration von cron-apt

Um unsere Updates automatisch installieren zu lassen, mÃ¼ssen wir **cron-apt** jetzt nur noch konfigurieren. Damit wird dann das Skript jeden Morgen um **4 Uhr Morgens** gestartet, und spielt die Updates ein. *(Die Uhrzeit kann noch geÃ¤ndert werden)*.

Wir Ã¶ffnen zuerst die Standardkonfiguration. Wir Ã¶ffnen die Datei **3-download** mit einem Editor unserer Wahl. Ich verwende hier *nano*.

```
sudo nano /etc/cron-apt/action.d/3-download
```

In dieser Datei befindet sich schon ein Befehl. Dieser Befehl wird automatisch ausgefÃ¼hrt, wenn, cron-apt gestartet wird. Dies geschieht dann automatisch, wenn die festgelegte Uhrzeit erreicht wird, oder wenn wir den Befehl `sudo cron-apt -s` eingeben.

Die Datei sollte folgenden Inhalt haben:

```
autoclean -y
dist-upgrade -d -y -o APT::Get::Show-Upgraded=true
```

Bei diesem Befehl werden die allgemeinen Updates nur heruntergeladen, aber nicht **installiert!** Wenn wir mÃ¶chten, dass die Updates automatisch installiert werden, mÃ¼ssen wir nur den Parameter **-d**entfernen. Dieser gibt an, dass die Updates nur heruntergeladen werden, und wir die Installation selbst in die Hand nehmen mÃ¼ssen.

Wenn die Updates automatisch installiert werden sollen, und man darÃ¼ber wegsieht, dass es dann zu Problemen kommen kann, durch beispielsweise zurÃ¼ckgezogene Pakete, kann man den nachstehenden Befehl anstelle des vorhandenen verwenden.

```
autoclean -y
dist-upgrade -y -o APT::Get::Show-Upgraded=true
```

Wenn wir beispielsweise wollen, dass die normalen Updates nicht automatisch installiert werden, aber Security Updates automatisch installiert werden sollen, kÃ¶nnen wir die DurchlÃ¤ufe durch eigene Skripte anpassen. Dazu mÃ¼ssen wir nur in demselben Verzeichnis eine Datei mit einer fortlaufenden Nummer und einer Beschreibung erstellen.

```
sudo nano /etc/cron-apt/action.d/10-securityupdates
```

In der Datei fÃ¼gen wir folgenden Inhalt ein:

```
upgrade -y -o APT::Get::Show-Upgraded=true
```

Damit jetzt unsere Datei auch verwendet wird, wenn **cron-apt** startet, mÃ¼ssen wir noch eine Konfigurationsdatei anlegen. Dazu legen wir wieder eine Datei mit dem Namen unser vorherigen angelegten Datei an. Dabei verÃ¤ndert sich nur der Ordner, in dem die Datei angelegt wird.

```
sudo nano /etc/cron-apt/config.d/10-securityupdates
```

Dort fÃ¼gen wir folgenden Code ein. Dabei mÃ¼ssen wir aber die entsprechenden Pfade zu den Paketquellen Listen angeben.

```
OPTIONS="-q -o Dir::Etc::SourceList=/etc/apt/sources.list.d/security.list -o Dir::Etc::SourceParts=\"/dev/null\""
```

AusfÃ¼hrungszeit Ã¤ndern

MÃ¶chten wir jetzt zuletzt noch Ã¤ndern, wann **cron-apt** ausgefÃ¼hrt wird, mÃ¼ssen wir die entsprechende Konfigurationsdatei Ã¶ffnen. Dazu verwenden wir den folgenden Befehl:

```
sudo nano /etc/cron.d/cron-apt
```

Wir kÃ¶nnen dort jetzt die Zeit angeben wann **cron-apt** ausgefÃ¼hrt werden soll. Die Zeit geben wir Ã¼ber Syntax der **Crontabs / Cronjobs** an.

Wenn wir jetzt Ã¼berprÃ¼fen wollen, ob unser Programm sauber durchlÃ¤uft, kÃ¶nnen wir es manuell starten, mit dem folgenden Befehl.

```
sudo cron-apt -s
```

Im Weiteren legt das Programm auch Logfiles ab. Diese kÃ¶nnen wir unter `/var/log/cron-apt` einsehen.

HTTPS Reverse Proxy mit Nginx konfigurieren

Einleitung

Sobald wir **Lokal Webdienste** erstellen, mÃ¶chten wir diese vielleicht auch Ã¼ber ein **TLS Zertifikat** verschlÃ¼sseln. Dazu verwenden wir **selbst signierte Zertifikate** und einen **Nginx Webserver**. Dadurch ist es mÃ¶glich, dass wir unsere **Web-Dienste** Ã¼ber **HTTPS** erreichbar machen kÃ¶nnen.

Wie wir **TLS Zertifikate** erstellen kÃ¶nnen, wird hier genauer erklÃ¤rt.

Nginx installieren

Im ersten Schritt mÃ¼ssen wir auf unserem **Debian Server** das Paket **Nginx** installieren. Dazu verwenden wir folgenden Befehl:

```
apt update && apt upgrade -y && apt install nginx -y
```

Nginx Konfiguration anpassen

Jetzt erstellen wir die **Nginx Konfigurationsdatei** einmal neu. Im Anschluss Ã¶ffnen wir die **Konfigurationsdatei** und fÃ¼gen den nachstehenden Inhalt in die Datei ein.

```
rm /etc/nginx/sites-enabled/default
nano /etc/nginx/sites-enabled/default
```

```
server {
  listen 80;
  server_name host.name;
  return 301 https://die.domain$request_uri;
 }

server {
  listen 443 ssl;
```

```
    server_name host.name;
    ssl_certificate  /pfad/zum/zertifikat.csr;
    ssl_certificate_key  /pfad/zum/zertifikat.key;
    ssl_prefer_server_ciphers on;

    location / {
        proxy_pass http://localhost:<port>;

        proxy_set_header        Host $host;
        proxy_set_header        X-Real-IP $remote_addr;
        proxy_set_header        X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header        X-Forwarded-Proto $scheme;
}
}
```

Sobald wir diesen Inhalt in die Datei eingefÃ¼gt haben, brauchen wir jetzt nur noch einmal den **Nginx Dienst** neu zu starten.

```
systemctl restart nginx
```

Sobald der Dienst neu gestartet ist, Ã¼berprÃ¼fen wir, ob der Dienst ordnungsgemÃ¤ÃŸ gestartet ist. Dies kÃ¶nnen wir mit dem nachstehenden Befehl Ã¼berprÃ¼fen.

```
systemctl status nginx
```

Nginx Reverse Proxy - WebSocket verliert die Verbindung

Einleitung

Konfigurieren wir unseren **Nginx Webserver** so, dass dieser als **Reverse Proxy** arbeitet, kÃ¶nnen wir bei einigen **Web-Anwendungen** das Problem haben, dass unser Client die Verbindung zum **WebSocket** verliert.

Konfiguration

Um dieses Problem zu beseitigen, mÃ¼ssen wir nur lediglich unsere **Nginx-Konfiguration** anpassen.

```
    location / {
        proxy_pass http://localhost:8080;

        proxy_http_version      1.1;
        proxy_set_header □□Upgrade $http_upgrade;
        proxy_set_header □□Connection "upgrade";
        proxy_set_header        Host $host;
        proxy_set_header        X-Real-IP $remote_addr;
        proxy_set_header        X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header        X-Forwarded-Proto $scheme;
□    }
```

Im Anschluss starten wir nur noch den **Nginx Webserver** neu. Danach sollte der **WebSocket** die Verbindung offen halten.

Apache2 SSL Virtualhost SSL Konfiguration

Einleitung

In diesem Beitrag befindet sich eine Version des **Apache2 Virtualhost** fÃ¼r die SSL Verbindung.

Konfigurationsdatei

```
  <VirtualHost *:80>
    ServerName FQDN
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html
    <Directory />
          Options FollowSymLinks
          AllowOverride None
    </Directory>
    ErrorLog  /error.log
    LogLevel warn
    CustomLog  /access.log combined
    ServerSignature On
</VirtualHost>

  <VirtualHost *:443>
    ServerName FQDN
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html

    <Directory />
          Options FollowSymLinks
          AllowOverride None
    </Directory>
    ErrorLog  /error.log
    LogLevel warn
```

```
    CustomLog  /access.log combined
    ServerSignature On
        SSLEngine on
        SSLCertificateFile /cert/cert.crt
        SSLCertificateKeyFile /cert/cert.key
</VirtualHost>
```

Service Konfiguration

E-Mail bei Linux Updates

Einleitung

In Linux kannst du mit Hilfe von **Apticron** automatisiert E-Mail Benachrichtigungen versenden wenn Updates verfÃ¼gbar sind. Du kannst dort auch einstellen das du informiert werden mÃ¶chtest, selbst wenn keine Updates verfÃ¼gbar sind.

Einrichtung

Im ersten Schritt verbindest du dich mit deinem Server damit du Konsolenzugriff hast. Dort aktualisierst du einmal die Paketquellen und installierst mÃ¶gliche Updates.

```
sudo apt update && sudo apt upgrade -y
```

Im nÃ¤chsten Schritt installierst du **Apticron** und **sendmail** auf deinem Rechner.

```
sudo apt install apticron sendmail -y
```

Als nÃ¤chstes kopierst du die Konfigurationsdatei in das Apticron Verzeichnis damit du diese modifizieren kannst.

```
sudo cp /usr/lib/apticron/apticron.conf /etc/apticron/apticron.conf
```

Diese Konfigurationsdatei Ã¶ffnest du in einem Editor deiner Wahl, ich verwende dazu **nano**.

```
nano /etc/apticron/apticron.conf
```

In dieser Datei gibst du Parameter an wie die E-Mail aussehen soll, welche Absender Adresse er verwenden soll und wer der EmpfÃ¤nger ist.

```
# apticron.conf
#
# The values set in /etc/apticron/apticron.conf will override the settings
# in this file.


#
# Set EMAIL to a space separated list of addresses which will be notified of
```

```
# impending updates. By default the root account will be notified.
#
EMAIL="<empfÃ¤nger>@<domain>"

#
# Set DIFF_ONLY to "1" to only output the difference of the current run
# compared to the last run (ie. only new upgrades since the last run). If there
# are no differences, no output/email will be generated. By default, apticron
# will output everything that needs to be upgraded.
#
# DIFF_ONLY="1"
#
DIFF_ONLY="0"

#
# Set LISTCHANGES_PROFILE if you would like apticron to invoke apt-listchanges
# with the --profile option. You should add a corresponding profile to
# /etc/apt/listchanges.conf
#
# LISTCHANGES_PROFILE="apticron"
#
# By default apt-listchanges is run with no profile
#
LISTCHANGES_PROFILE=""

#
# From hostname manpage: "Displays  all FQDNs of the machine. This option
# enumerates all configured network addresses on all configured network interâ€
# faces, and translates them to DNS domain names. Addresses that cannot be
# translated (i.e. because they do not have an appropriate  reverse DNS
# entry) are skipped. Note that different addresses may resolve to the same
# name, therefore the output may contain duplicate entries. Do not make any
# assumptions about the order of the output."
#
# By default only the first FQDN is used
#
# ALL_FQDNS="1"
ALL_FQDNS="0"

#
```

```
# Set SYSTEM if you would like apticron to use something other than the output
# of "hostname -f" for the system name in the mails it generates. This option
# overrides the ALL_FQDNS above.
#
# SYSTEM="foobar.example.com"
#
SYSTEM="<FQDN>"

#
# Set IPADDRESSNUM if you would like to configure the maximal number of IP
# addresses apticron displays. The default is to display 1 address of each
# family type (inet, inet6), if available.
#
IPADDRESSNUM="1"

#
# Set IPADDRESSES to a whitespace separated list of reachable addresses for
# this system. If unset or empty, apticron will try to work these out using
# the "ip" command.
#
# IPADDRESSES="192.0.2.1 2001:db8:1:2:3::1"
#
IPADDRESSES=""

#
# Set NOTIFY_HOLDS="0" if you don't want to be notified about new versions of
# packages on hold in your system. The default behavior is downloading and
# listing them as any other package.
#
# NOTIFY_HOLDS="0"
#
NOTIFY_HOLDS="1"

#
# Set NOTIFY_NEW="0" if you don't want to be notified about packages which
# are not installed in your system. Yes, it's possible! There are some issues
# related to systems which have mixed stable/unstable sources. In these cases
# apt-get will consider for example that packages with "Priority:
# required"/"Essential: yes" in unstable but not in stable should be installed,
# so they will be listed in dist-upgrade output. Please take a look at
```

```
# http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=531002#44
#
# NOTIFY_NEW="0"
#
NOTIFY_NEW="1"

#
# Set NOTIFY_NO_UPDATES="1" if you want to be notified when there are no
# new versions. This is useful to assure you that apticron works well.
# By default notifications will be sent only when new versions are available.
#
# NOTIFY_NO_UPDATES="1"
#
NOTIFY_NO_UPDATES="1"

#
# Set CUSTOM_SUBJECT if you want to replace the default subject used in
# the notification e-mails. This may help filtering/sorting client-side e-mail.
# If you want to use internal vars please use single quotes here. Ex:
CUSTOM_SUBJECT='[apticron] $SYSTEM: $NUM_PACKAGES package update(s)'
#
# CUSTOM_SUBJECT=""

#
# Set CUSTOM_NO_UPDATES_SUBJECT if you want to replace the default subject used
# in the no update notification e-mails. This may help filtering/sorting
# client-side e-mail.
# If you want to use internal vars please use single quotes here. Ex:
CUSTOM_NO_UPDATES_SUBJECT='[apticron] $SYSTEM: no updates'
#
# CUSTOM_NO_UPDATES_SUBJECT=""

#
# Set CUSTOM_FROM if you want to replace the default sender by changing the
# 'From:' field used in the notification e-mails.
#
 CUSTOM_FROM="<sender>@<domain>"

# Set GPG_ENCRYPT="1" if you want to encrypt the mail being send to
# $EMAIL. apticron will use gpg and the public key of the recipient to encrypt
```

```
# the mail. Please note that the $EMAIL value above can't be an alias, since
# gpg will trust it to encrypt the message.
#
GPG_ENCRYPT="0"
```

Apticron verwendet immer die Datei im **/etc/apticron** Verzeichnis wenn diese existiert. Sonst nutzt er die aus dem **/usr/lib/apticron** Verzeichnis.

Wenn du Ã¼berprÃ¼fen mÃ¶chtest ob **Apticron** funktioniert, setze folgenden Befehl ab.

```
sudo apticron
```

E-Mail Benachrichtigung bei SSH Login

Einleitung

Wenn wir einen Linux Server absichern wollen, gehÃ¶rt eine stetige Kontrolle aus SicherheitsgrÃ¼nden auch dazu. Hier konfigurieren wir eine E-Mail Benachrichtigung die abgesendet wird sobald sich jemand per SSH auf dem Server einloggt.

DurchfÃ¼hrung

Zuerst mÃ¼ssen wir das Paket **s-nail** installieren.

```
sudo apt install s-nail -y
```

Im zweiten Schritt erstellen wir ein Skript welches ausgefÃ¼hrt wird sobald sich jemand auf dem Server einloggt.

```
nano /opt/skripte/ssh-login.sh
```

Dort fÃ¼gen wir folgenden Inhalt ein, das Skript kann natÃ¼rlich auch gerne angepasst werden.

```
#!/bin/bash
echo "------------------------------------------------------------------"
echo "Login auf $(hostname) am $(date +%Y-%m-%d) um $(date +%H:%M)"
echo "Benutzer: $USER"
echo "------------------------------------------------------------------"
pinky
```

Jetzt verÃ¤ndern wir die Datei **/etc/profile** und fÃ¼gen dort den Aufrufer des Skriptes hinzu

```
/opt/skripte/ssh-login.sh | mailx -s "SSH Login auf <server>" <empfÃ¤nger>@<domain>
```

Als letztes passen wir noch die Berechtigungen des Skriptes an.

```
sudo chmod 755 /opt/skripte/ssh-login.sh
```

Die E-Mails werden jetzt bei einer Anmeldung automatisch an die entsprechende E-Mail Adresse versendet.

Port von sendmail Ã¤ndern

Einleitung

Manchmal stÃ¶ÃŸt man auf folgendes Problem: Auf einem Server lÃ¤uft ein Mailserver, z.B. in einem Docker Container und dazu mÃ¶chte man mit **sendmail** ggf. Mails versenden. Dazu mÃ¼ssen wir den Port von **sendmail** verÃ¤ndern.

Anwendung

Zuerst verbinden wir uns mit unseren Server damit wir Konsolenzugriff haben. Dort Ã¶ffnen wir mit einem Editor unserer Wahl die Konfigurationsdatei.

```
sudo nano /etc/mail/sendmail.mc
```

Dort suchen wir nach folgenden Zeilen:

```
dnl DAEMON_OPTIONS(`Family=inet6, Name=MTA-v6, Port=smtp, Addr=::1')dnl
DAEMON_OPTIONS(`Family=inet,  Name=MTA-v4, Port=smtp, Addr=127.0.0.1')dnl
```

Dort ersetzt du **smtp** durch die Port Nummer deiner Wahl.

```
dnl DAEMON_OPTIONS(`Family=inet6, Name=MTA-v6, Port=25000, Addr=::1')dnl
DAEMON_OPTIONS(`Family=inet,  Name=MTA-v4, Port=25000, Addr=127.0.0.1')dnl
```

Als nÃ¤chstes lÃ¤sst du dir die Konfigurationsdatei neu erstellen.

```
sudo m4 /etc/mail/sendmail.mc > /etc/mail/sendmail.cf
```

Und als letztes startest du sendmail neu, dann sollte dein sendmail jetzt den neuen Port verwenden.

```
sudo systemctl restart sendmail
```

SSH Root Login verbieten

Einleitung

Damit wir einen sicheren Linux Server haben, kÃ¶nnen wir den Root Zugang Ã¼ber SSH auf unserem Server deaktivieren. Wenn Server angegriffen werden, wird zuerst immer der **root** Benutzer verwendet da dieser auf jedem System eingerichtet ist und volle Berechtigungen hat.

Login deaktivieren

Um den Root Login zu deaktivieren, mÃ¼ssen wir die Konfigurationsdatei des SSH Services editieren. Dazu navigieren wir in das Verzeichnis vom SSH Dienst.

```
cd /etc/ssh
```

Dort Ã¶ffnen wir mit dem Editor unserer Wahl die Konfigurationsdatei.

```
nano sshd_config
```

Dort mÃ¼ssen wir nach **PermitRootLogin** suchen. Wir mÃ¼ssen dort eine Raute vor den Eintrag hinzufÃ¼gen damit dieser aus kommentiert ist.

Dann starten wir den SSH Server neu.

```
sudo systemctl restart ssh
```

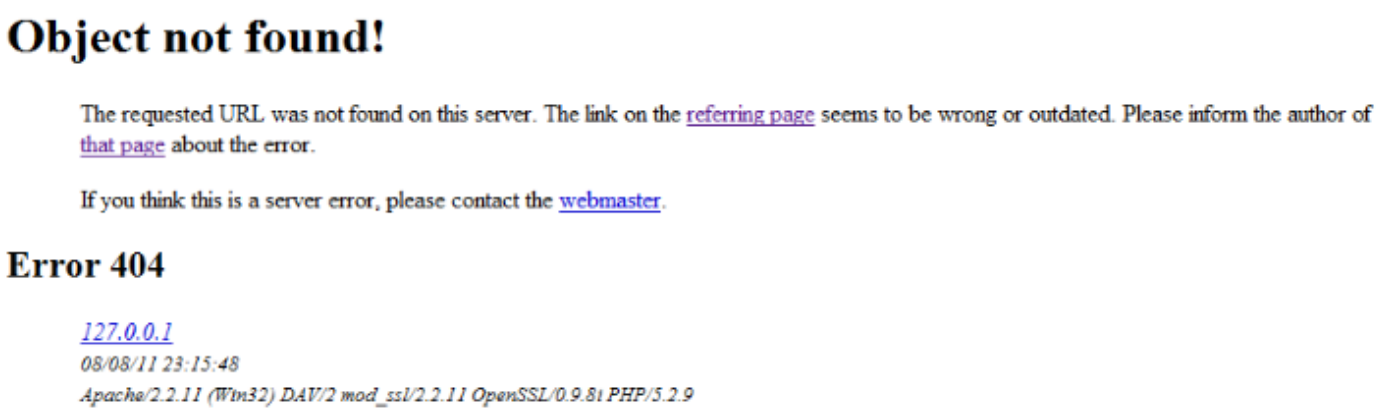
Jetzt ist kein Login als Root mehr mÃ¶glich!

> Stelle vorher sicher das ein weiterer Benutzer angelegt ist, mit dem man sich weiterhin am Server anmelden kann.

Apache - Error 404 "Objekt nicht gefunden"

Einleitung

In diesem Beitrag erlÃ¤utere ich kurz, wie wir das Problem mit dem **Apache Fehler 404 "Objekt nicht gefunden"**, beheben kÃ¶nnen. Das Problem kann mehrere Ursachen habe, aber diese, die mir aktuell untergekommen sind, zÃ¤hle ich hier auf.



Fehler beheben

1. Berechtigungen falsch gesetzt

Ein Fehler kann es sein, dass es nicht mÃ¶glich ist aufgrund fehlender Berechtigungen die Webserver Dateien anzuzeigen. Zu Testzwecken kÃ¶nnen wir ruhig mal die Berechtigung auf **777** setzen. In Produktivumgebungen sollten die Berechtigungen so gesetzt werden, dass nur die Berechtigungen eingerÃ¤umt werden, welche benÃ¶tigt werden.

Zu den, wie oben angegebenen Testzwecken kann man es mit diesen Berechtigungen mal ausprobieren, ob es dann funktioniert.

```
chmod 777 -R /pfad/zum/webroot
```

Wir kÃ¶nnen dann auch noch den Besitzer der Dateien / Ordner Ã¤ndern. Apache verwendet Standard-gemÃ¤ÃŸ den Benutzer *www-data*. Diesem Benutzer werden wir gleich die Besitzerrechte des Ordners verpassen. Dieser kann dann alles mit dem Verzeichnis anstellen.

```
chown -R www-data:www-data /pfad/zum/webroot
```

2. Fehlende .htaccess Datei

Ein kleiner, aber dennoch tragischer Fehler kann eine fehlende .htaccess Datei sein. Manchmal kann es bei einem Kopiervorgang vorkommen, dass wir vergessen die **.htaccess** Datei mitzukopieren. Falls diese fehlt, kann der Webserver manchmal Webserver Dateien nicht Ã¶ffnen oder PHP-Skripte ausfÃ¼hren.

Die **.htaccess** Datei enthÃ¤lt Anweisungen fÃ¼r den Apache-Webserver. Ohne diese Datei kann ein Apache Webserver z.B. nicht mit *Redirects* umgehen.

Terminal Befehle

Arbeitsspeicher im Cache freigeben

Einleitung

Wenn du einen Linux Server lÃ¤nger in Betrieb hast, kann es sein das dein Monitoring System anschlÃ¤gt und meldet das kein Arbeitsspeicher mehr frei ist. Der Arbeitsspeicher befindet sich dennoch nur im Cache.

> DurchfÃ¼hrung geschieht auf eigene Gefahr!

ErklÃ¤rung

Wenn ein Linux System arbeitet, schreibt das System hÃ¤ufig verwendete Dateien und Daten in den Cache. So muss nicht immer die Festplatte verwendet werden. Dieses ermÃ¶glicht eine hÃ¶here Geschwindigkeit des Servers.

Der Cache beeintrÃ¤chtigt das Linux System aber nicht weiter, wenn das Linux System merkt das es mehr Arbeitsspeicher braucht, gibt es automatisch mehr Arbeitsspeicher frei.

Befehl

Mithilfe des folgenden Befehls wird der Cache wieder freigegeben. Der Server nimmt dann nur den Arbeitsspeicher den er momentan braucht.

```
sync && echo 3 > /proc/sys/vm/drop_caches
```

Falls du sehen mÃ¶chtest wie sich die Auslastung des Arbeitsspeichers verÃ¤ndert, kannst du jeweils ein `free` ansetzen. Dieses zeigt an wie viel Arbeitsspeicher der Server gesamt, benutzt und frei hat. Dieses wird dann wieder in den Hauptspeicher und SWAP aufgegliedert.

```
free && sync && echo 3 > /proc/sys/vm/drop_caches && free
```

ErklÃ¤rung Befehl

Der `free` Befehl sorgt dafÃ¼r eine RÃ¼ckmeldung Ã¼ber den freien, verwendeten und gesamten Arbeitsspeicher anzuzeigen.

`sync` schreibt die Cache Dateien auf die Festplatte.

`echo 3 > /proc/sys/vm/drop_caches` schreibt die Zahl 3 in die Datei **drop_caches** was zur Folge hat, das der Cache wieder freigegeben wird.

Linux Version anzeigen lassen

Einleitung

Es gibt mehrere Wege die aktuelle Linux Version anzeigen zu lassen. Alle Wege die vorgestellt werden, werden Ã¼ber das Terminal durchgefÃ¼hrt. So kannst du diese auch ausfÃ¼hren wenn du Ã¼ber SSH / Telnet mit dem Server verbunden bist.

Linux Version und die Distribution anzeigen

Wenn du die Linux Version und die Distribution anzeigen lassen mÃ¶chtest, musst du einen entsprechenden Befehl absetzen. Diesen Befehl kannst du so gut wie auf jedem Linux System eingeben.

```
cat /etc/issue
```

Linux Installation 32 oder 64-bit?

Wenn du jetzt herausfinden mÃ¶chtest ob es sich bei der Linux Installation um eine 32 oder 64-bit Version handelt, kannst du den entsprechenden Befehl absetzen. Dieser gibt dir ein paar Grundinformationen Ã¼ber das System aus. Unter anderem die entsprechende Befehlssatz Architektur.

```
uname -a
```

Linux Systeminformation Ã¼bersichtlich darstellen

Als letztes kannst du die Systeminformationen dir schÃ¶n darstellen lassen. Dazu verwenden wir das Tool **neofetch**. Dieses musst du erst nachinstallieren.

Ubuntu

```
sudo add-apt-repository ppa:dawidd0811/neofetch
sudo apt-get update
sudo apt-get install neofetch -y
```

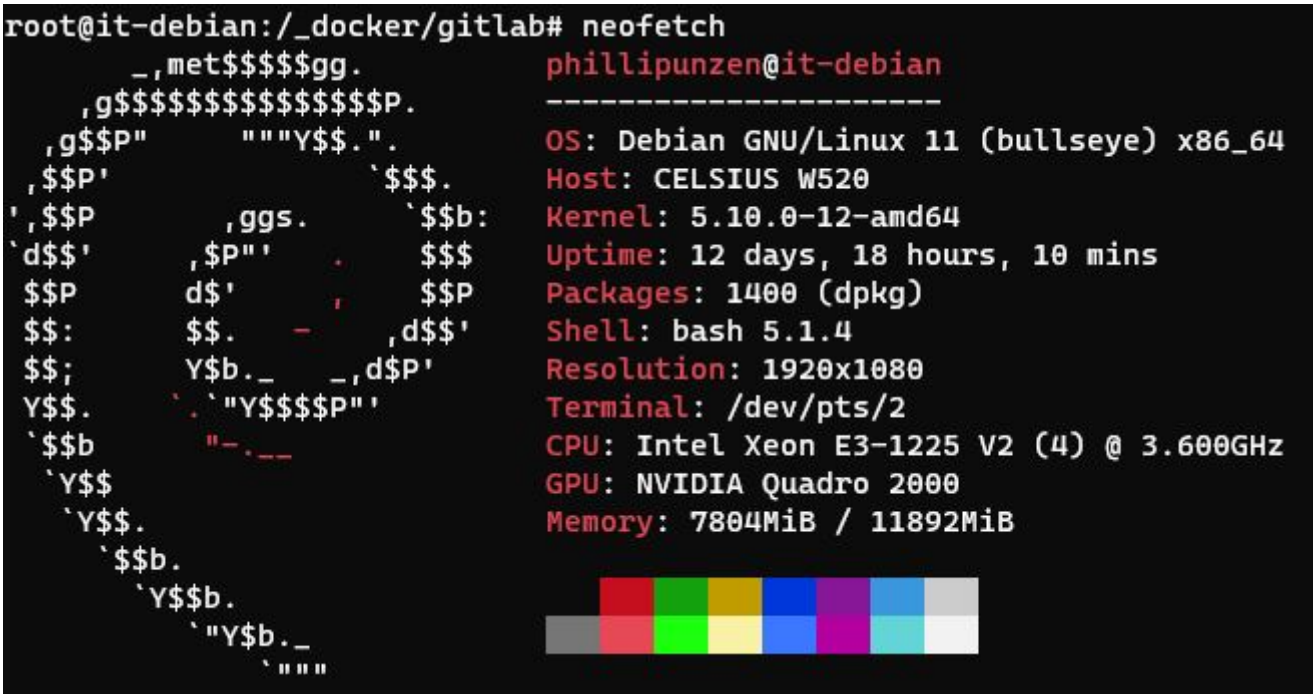
Debian

```
sudo apt-get install neofetch
```

Fedora

```
sudo dnf install neofetch
```

Wenn du das Tool nun installiert hast, kannst du mit dem Befehl `neofetch` dir die Systeminformationen anzeigen lassen.



Mit sendmail Mails verschicken

Einleitung

Es ist mÃ¶glich mit Linux Mails direkt aus der Kommandozeile zu versenden. Administratoren oder Programmierer schicken sich damit hÃ¤ufig Status Meldungen oder andere Nachrichten. Auf vielen Webseiten wird hÃ¤ufig dazu die PHP Funktion **sendmail** verwendet. Dazu brauchst du einen E-Mail Account bei einem Provider deiner Wahl. Wenn der Mail-Server im gleichen Netz wie der Web Server steht, und keine Kommunikation Ã¼ber das Internet erfolgen muss, kann bei richtiger Kommunikation ohne einen E-Mail Account, eine E-Mail versendet werden.

> sendmail gilt als veraltet und sollte dementsprechend mit Bedacht verwendet werden.

Voraussetzungen

Um jetzt E-Mails mit sendmail Ã¼ber das Internet zu versenden benÃ¶tigst du folgende Informationen zu deinem E-Mail Account:

- SMTP-Adresse
- SMTP-Port
- Login Daten (Benutzername und Kennwort)

E-Mail versenden

Wenn du E-Mails versenden mÃ¶chtest kannst du das Ã¼ber unterschiedliche MÃ¶glichkeiten machen. Alle gehen direkt von der Kommandozeile aus. Du musst also keine GUI oder sonstige Web OberflÃ¤che Ã¶ffnen.

Du benÃ¶tigst um E-Mails zu versenden das Paket **ssmtp**. Dieses kÃ¶nnen wir einfach nachinstallieren.

```
sudo apt install ssmtp -y
```

E-Mail nur mit Betreff

```
echo "Subject: Test E-Mail" | sendmail mail@pc-wiki.de
```

E-Mail aus Datei lesen

Zuerst legen wir eine Datei an in dem sich der E-Mail Inhalt befindet.

```
nano email.txt
```

In dieser Textdatei fÃ¼gst du den Text ein, den du gerne versenden mÃ¶chtest. Den Betreff, E-Mail Adressen und den Nachrichten Text kannst du natÃ¼rlich gerne Ã¤ndern. Wichtig ist, das die Struktur so bestehen bleibt.

```
Cc: mail@phil-un.de
Subject: E-Mail aus Datei
From: server@pc-wiki.de
Content-Type: text/html; charset="utf8"

<html>
<body>
<div style="
background-color:
#abcdef; width: 300px;
height: 300px;
">
</div>
  <h1>Status Meldung</h1>
  <p>Die E-Mails werden erfolgreich vom Server versendet!</p>
</body>
</html>
```

Zum Schluss mÃ¼ssen wir nur noch die E-Mail versenden. Dort kannst du den EmpfÃ¤nger natÃ¼rlich wieder anpassen.

```
sendmail mail@pc-wiki.de < mail.txt
```

E-Mail Ã¼ber STMP Server versenden

Wenn du E-Mails Ã¼ber den SMTP Server versenden mÃ¶chtest, um z.B. E-Mails Ã¼ber einen E-Mail Server zu versenden. Musst du die Login Daten in einer Konfigurationsdatei angeben. Ã–ffne zuerst die Konfigurationsdatei

```
sudo nano /etc/ssmtp/ssmtp.conf
```

Dort fÃ¼gst du folgenden Code ein. Die Login Daten sowie den Mail Server musst du noch anpassen.

```
UseSTARTTLS=YES
root=server@phil-un.de
mailhub=mail.server.de:587
AuthUser=<server>
AuthPass=<Pa$$w0rd>
```

Und nun versendest du eine E-Mail mit dem folgenden Befehl

```
ssmtp mail@pc-wiki.de < mail.txt
```

> Wenn eine Fehlermeldung erscheint, kannst du diese nutzen um den Fehler zu finden.
> **Beispiel:** `ssmtp: Authorization failed`

Skript ausfÃ¼hrbar machen

Einleitung

In Linux kannst du grundlegend fremde Skripte nicht starten. Diese musst du dann quasi erst freigeben, dann kÃ¶nnen die Skripte ausgefÃ¼hrt werden.

Skript freigeben

Wenn du ein Skript ausfÃ¼hrbar machen mÃ¶chtest, wechselst du in das Verzeichnis in dem sich das Skript befindet und setzt dann den Namen der Datei an das Ende. Dann kannst du das Skript ohne Probleme ausfÃ¼hren.

```
sudo chmod +x ./<name-des-skripts>
```

Belegte Ports in Linux ausgeben

Einleitung

In diesem Beitrag beschreibe ich kurz, wie wir unter Linux uns ausgeben lassen kÃ¶nnen, welche Software oder Dienst einen bestimmten Port belegt. Dies ist wichtig, wenn, wie z. B.Starten einen neuen Dienst installieren mÃ¶chten und wir beim Starten die Meldung erhalten, dass der Port belegt ist. Damit kÃ¶nnen wir dann feststellen, was die Ursache dafÃ¼r ist.

Ursache herausfinden

Um die Ursache herauszufinden, warum ein Port schon verwendet ist, mÃ¼ssen wir nur das **Terminal / Konsole** Ã¶ffnen und den folgenden Befehl eingeben. Dabei mÃ¼ssen wir nur `<Port>` durch die **Port Nummer** ersetzen. Wir erhalten dann eine Liste aller Anwendungen, die diesen Port nutzen.

```
ss -tunelp | grep <port>
```

CPU Informationen und Auslastung im Terminal anzeigen

Einleitung

In diesem Beitrag erklÃ¤re ich kurz, wie wir in einem Linux Terminal einsehen kÃ¶nnen, welche CPU in unserem System verbaut ist, und wie die Auslastung der entsprechenden CPU ist.

CPU-Informationen anzeigen

Damit wir die CPU Informationen anzeigt bekommen, mÃ¼ssen wir den folgenden Befehl eingeben.

```
sudo cat /proc/cpuinfo | less
```

Wir erhalten jetzt die CPU Informationen pro Kern. Das heiÃŸt, entsprechend wie viele Kerne wir haben, bekommen wir so oft die Ausgabe in das Konsolenfenster ausgegeben. Mit der Taste **Q** schlieÃŸen wir die Ansicht.

Erweiterte CPU-Informationen anzeigen

Wenn wir erweiterte CPU-Informationen angezeigt bekommen mÃ¶chten, mÃ¼ssen wir den Befehl `lscpu` verwenden. Dieser gibt in der Konsole eine erweiterte Ansicht Ã¼ber die CPU Informationen dar.

```
sudo lscpu
```

CPU Auslastung anzeigen

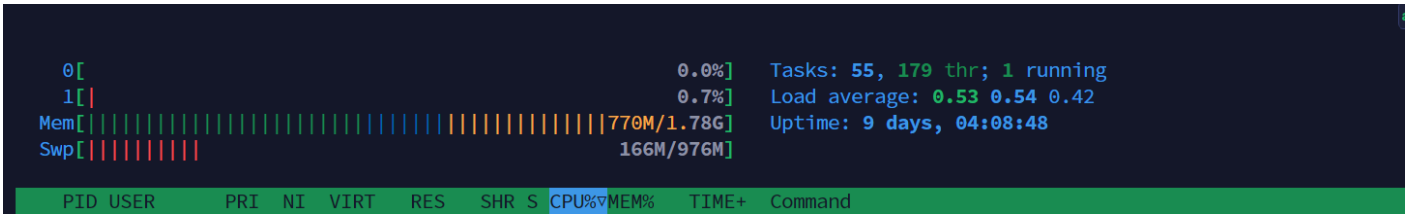
Um die CPU Auslastung unseres Linux Servers uns anzeigen zu lassen, kÃ¶nnen wir das Tool **htop** verwenden. Dieses kann man schnell Ã¼ber den Paketmanager nachinstallieren.

Installation fÃ¼r **Debian / Ubuntu** sieht wie folgt aus:

```
sudo apt install htop -y
```

Nach der erfolgreichen Installation kÃ¶nnen wir durch den Befehl `sudo htop` das Tool Ã¶ffnen. Wir erhalten dann eine detaillierte Ãœbersicht Ã¼ber die verfÃ¼gbaren Kerne und deren einzelnen Auslastung.

```
sudo htop
```



Hostnamen des Rechners / Servers Ã¤ndern

Einleitung

In diesem Beitrag erlÃ¤utere ich kurz, wie wir unter **Linux** den **Hostnamen** unseres **Rechners / Servers** Ã¤ndern kÃ¶nnen. Dieser ist fÃ¼r **DNS AuflÃ¶sungen** z.B. relevant.

Hostnamen Ã¤ndern

Um den **Hostnamen** zu Ã¤ndern, mÃ¼ssen wir lediglich ein Terminal Fenster Ã¶ffnen und dort mit einem Benutzer anmelden, der `sudo` Privilegien besitzt.

Sobald wir dies getan haben, geben wir den nachstehenden Befehl ein. Dabei mÃ¼ssen wir nur den gewÃ¼nschten **Hostnamen** in den Befehl eingeben.

```
sudo hostnamectl set-hostname <hostname>
```

DNS auf Linux Rechner deaktivieren

Einleitung

Bei der Installation eines DNS-Servers kannes erforderlich sein, das der vorhandene DNS-Dienst deaktiviert werden muss.

Dienst deaktivieren

DafÃ¼r mÃ¼ssen wir nur den nachstehenden Code eingeben:

```
sudo systemctl disable systemd-resolved
sudo systemctl stop systemd-resolved
```

Mit MariaDB-Client auf einen anderen SQL-Server verbinden

Einleitung

Neulich bin ich auf das Thema gestoÃŸen, wie ich mithilfe des **MariaDB-Clients,** welchen ich unter Debian mit `apt-install mariadb-client -y` installieren kann, auf einen anderen SQL-Server mich verbinden kann. Hintergrund war die Installation von **Zabbix** auf einem anderen MariaDB-Server.

Mit SQL-Server verbinden

Um die Verbindung durchzufÃ¼hren, muss im Terminal nur der folgende Befehl eingegeben werden:

```
mysql -h <host> -u <user> -p <datenbank>
```

Es wird im Anschluss nach dem Kennwort fÃ¼r den Benutzer gefragt. Sobald dieses richtig eingegeben wurde, erscheint die **SQL-Shell** des entfernten Systems. Jetzt kÃ¶nnen wir Befehle auf unserer Datenbank absetzen.

Verzeichnis und Dateien in ein ZIP-Archiv verschieben

Einleitung

In dieser Anleitung beschreibe ich kurz, wie wir unter Linux **Dateien** und **Verzeichnisse** in ein **ZIP-Archiv** verpacken kÃ¶nnen. SO kÃ¶nnen wir die Dateien schneller zwischen Servern verschieben oder die Datenmengen verkleinern.

ZIP-Archiv erstellen

Paket installieren

Unter UmstÃ¤nden kann es sein, dass das benÃ¶tigte Paket zum Erstellen von ZIP-Archiven noch nicht auf dem Betriebssystem installiert ist. DafÃ¼r setzen wir den nachstehenden Befehl ab:

```
apt install zip -y
```

Dateien verpacken

Um jetzt Dateien zu verpacken, setzen wir den folgenden Befehl ab. Wir mÃ¼ssen dort nur die Dateinamen anpassen.

```
zip <ziel.zip> <DATEI1> <DATEI2> <DATEI3>
```

Ordner verpacken

Um Ordner zu verpacken, mÃ¼ssen wir den Befehl nur um den Parameter **-r** erweitern.

```
zip <ziel.zip> -r <pfad-zum-ordner>
```

Kompressionslevel Ã¤ndern

Wir kÃ¶nnen auch die **Kompression** erhÃ¶hen, um die DateigrÃ¶ÃŸe herunterzudrÃ¼cken. Dabei kÃ¶nnen wir von Level **1 - 9** wechseln. Je hÃ¶her das Level, desto kleiner wird die Datei, aber desto lÃ¤nger dauert der Vorgang.

```
zip <ziel.zip> -9 -r <pfad-zur-datei>
```

Archiv mit Kennwort schÃ¼tzen

Es ist auch mÃ¶glich, das Verzeichnis mit einem Kennwort zu schÃ¼tzen. Dazu ergÃ¤nzen wir den Befehl um ein **-e**.

```
zip -e -r <ziel.zip> <pfad-zum-ordner>
```

Partition von Debian im laufenden Betrieb vergrÃ¶ÃŸern

Einleitung

In dieser Anleitung vergrÃ¶ÃŸern wir die vorhandene Debian Partition auf das Maximum. So kÃ¶nnen wir die Daten-Partition unseres Servers vergrÃ¶ÃŸern, um mehr Daten auf der Festplatte abzulegen. Dies ist besonders vorteilhaft in Virtualisierungsumgebungen.

> **WICHTIG!** Es sollte vorher in jedem Fall ein Backup vom Server gemacht werden! Unter UmstÃ¤nden kann die VerÃ¤nderung der Partition zu Datenverlust fÃ¼hren!

Partition vergrÃ¶ÃŸern

Im ersten Schritt mÃ¼ssen wir mit **fdisk** die Festplatte "Ã¶ffnen":

```
sudo fdisk /dev/sda
```

Im nÃ¤chsten Schritt arbeiten wir die Abfragen ab. Bei mir sieht das wie folgt aus:

```
WARNING: DOS-compatible mode is deprecated. It's strongly recommended to
        switch off the mode (command 'c') and change display units to
        sectors (command 'u').

Command (m for help): d
Selected partition 1

Command (m for help): n
Command action
   e   extended
   p   primary partition (1-4)
```

```
p
Partition number (1-4): 1
First cylinder (1-83220, default 1): 64
Last cylinder, +cylinders or +size{K,M,G} (63-83220, default 83220): 83220

Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.
Syncing disks.
```

Sobald das abgeschlossen ist, kÃ¶nnen wir mit dem Befehl `lsblk` Ã¼berprÃ¼fen, ob die Erweiterung erfolgreich durchgefÃ¼hrt wurde.

GRUB Bootloader

Standard Boot Partition Ã¤ndern

Einleitung

In diesem Beitrag gehe ich drauf ein, wie wir beim GRUB Bootloader die Standard-Partition, die zum Booten verwendet wird, Ã¤ndern kÃ¶nnen. Durch die Ã„nderung wÃ¼rde das System, wenn es keine andere Eingabe erhÃ¤lt, automatisch das entsprechende Betriebssystem starten.

Boot Reihenfolge Ã¤ndern

Backup erstellen

Im ersten Schritt erstellen wir ein Backup unserer derzeitigen GRUB Konfiguration. Dies empfiehlt sich, da Ã„nderungen am Bootloader auch zu Problemen fÃ¼hren kann. Und so kÃ¶nnen wir jederzeit wieder zurÃ¼ck auf die vorherige Konfiguration.

Um ein Backup zu erstellen, fÃ¼hre den folgenden Befehl aus:

```
sudo cp /etc/default/grub /etc/default/grub.bak
```

Ps: Wir kÃ¶nnen natÃ¼rlich auch einen anderen Zielnamen Ã¼berlegen, falls wir z.B. schon eine Datei mit dem Namen haben, welche nicht Ã¼berschrieben werden soll.

Backup kontrollieren

Um sicherzustellen, dass der Backup-Vorgang erfolgreich durchgefÃ¼hrt wurde, fÃ¼hren wir den folgenden Befehl aus, um uns den Dateiinhalt der Datei anzeigen zu lassen.

```
cat /etc/default/grub.bak
```

Ã„nderungen speichern

Um einmal die Ã„nderungen zu registrieren, fÃ¼hren wir den folgenden Befehl aus:

```
sudo update-grub
```

Damit wird noch einmal die aktuelle GRUB Konfiguration in den Bootloader geschrieben. Jetzt werden wir aber die Ã„nderungen durchfÃ¼hren und werden dementsprechend den Befehl nachher nochmal ausfÃ¼hren.

Ã„nderungen vornehmen

Um die Ã„nderungen an der Datei vorzunehmen, mÃ¼ssen wir mit einem Editor unserer Wahl die GRUB Konfigurationsdatei Ã¶ffnen. Ich verwende dafÃ¼r den Terminal Editor **nano**.

```
sudo nano /etc/default/grub
```

Hier mÃ¼ssen wir nur die Zahl hinter GRUB_DEFAULT= Ã¤ndern. Hier geben wir die Position des Boot Eintrags ein, welchen wir verwenden mÃ¶chten. Die AufzÃ¤hlung beginnt bei 0. Sprich: Die erste Position ist 0, die zweite Position ist 1, und immer so weiter.

Sobald wir die Ã„nderungen durchgefÃ¼hrt haben, mÃ¼ssen wir wieder den GRUB Bootloader aktualisieren. Dabei wird dann die aktuelle Konfigurationsdatei eingelesen.

```
sudo update-grub
```

Bootloader Hintergrund Ã¤ndern

Einleitung

In diesem Beitrag gehe ich kurz drauf ein, wie wir im GRUB Bootloader das Hintergrundbild des Bootloaders Ã¤ndern kÃ¶nnen.

Bild Ã¤ndern

Dazu mÃ¼ssen wir einfach ein Bild, welches wir uns heruntergeladen haben, in ein Verzeichnis kopieren / verschieben. Diesen Pfad mÃ¼ssen wir uns jetzt merken oder aufschreiben.

```
sudo cp index.jpeg /boot/grub/
```

Im Anschluss Ã¶ffnen wir wieder die GRUB Konfigurationsdatei und fÃ¼gen folgenden Code mit unserem Pfad hinzu.

```
GRUB_BACKGROUND="/boot/grub/index.jpeg"
```

Am Schluss mÃ¼ssen wir jetzt nur die GRUB Konfiguration wieder aktualisieren.

```
sudo update-grub
```

Problembeseitigung

Problembeseitigung

Debian Fehlermeldung: dpkg: warning: 'ldconfig' not found in PATH or not executable.

Einleitung

Letztens bin ich bei der Installation eines Linux Servers auf folgendes Problem gestoÃŸen.
Beim Installieren von Paketen bekam ich die oben angegebenen Fehlermeldung:

> dpkg: warning: 'ldconfig' not found in PATH or not executable

In diesem Beitrag will ich kurz zeigen, wie wir das Problem beseitigen kÃ¶nnen.

Problem beseitigen

Im ersten Schritt mÃ¼ssen wir uns per **SSH** auf unseren Linux Server schalten, oder anderweitig den **Shell-Zugriff** erreichen. Im Anschluss geben wir die nachstehende Befehle nacheinander ein:

```
nano /root/.bashrc
```

Dort fÃ¼gen wir in der letzten Zeile der Datei den folgenden Code ein und speichern die Datei:

```
export PATH=/sbin:/bin:/usr/bin:/usr/sbin:/usr/local/sbin:/usr/local/bin
```

Als letzten Schritt geben wir den folgenden Befehl ein:

```
. /root/.bashrc
```

Jetzt sollte es mÃ¶glich sein, die Pakete wieder zu installieren!

Wireguard

Wireguard Client auf Debian installieren

Einleitung

In dieser Anleitung beschreibe ich kurz, wie in **Debian** einen **Wireguard Client** installieren und konfigurieren. Damit kÃ¶nnen wir eine **VPN-Verbindung** herstellen.

Wireguard Client

Im ersten Schritt installieren wir das benÃ¶tigte Paket.

```
sudo apt -y install wireguard-tools
```

Im zweiten Schritt Ã¶ffnen wir die Konfigurationsdatei und fÃ¼gen dort den Inhalt der Konfiguration ein.

```
[Interface]
# specify private key for client generated on WireGuard server
PrivateKey = 0PSYJtK2MtCx3GA0MEvEiuq3AiRLH8qqwRCupcO4A2M=
# IP address for VPN interface
Address = 172.16.1.5

[Peer]
# specify public key for server generated on WireGuard server
PublicKey = Q55BcMribgGGRJo4e1jDhEbXZyLPnLeMnMLAcRVsHVg=
# IP addresses you allow to connect
# on the example below, set WireGuard server's VPN IP address and real local network
AllowedIPs = 172.16.1.1, 10.0.0.0/24
# specify server's global IP address:port
# (acutually, example of IP below is for private range, replace to your own global IP)
EndPoint = 172.16.1.100:51820
```

Zum Schluss starten wir jetzt die Netzwerkkarte mit der Wireguard Konfiguration.

```
wg-quick up wg0
```