# Server Installationsanleitung

## Betriebssystem Installation

* Das Image von raspberry.com herunterladen und extrahieren. (<https://www.raspberrypi.org/downloads/raspbian/>)
* Um die Image auf der SD Karte zu bringen benutzt man Etcher. (<https://etcher.io/>)
* Mit den Standard-Anmeldedaten Anmelden. User: pi Password: raspberry
* System aktualisieren: sudo apt-get update & sudo apt-get upgrade
* SSH aktivieren:
  + sudo raspi-config in ein Terminal eingeben.
  + Interfacing Options auswählen.
  + SSH auswählen -> aktivieren.

## Software Installation

Nun werden die benötigten Dienste und Tools installiert, die von dem Server benötigt werden.

* Installation der Webserver. (PHP, Apache, MySQL, Java SDK, Composer, Utils)

sudo apt-get install apache2 apache2-doc apache2-utils

sudo apt-get install libapache2-mod-php5 php5 php-pear php5-xcache  
sudo apt-get install php5-mysql

sudo apt-get install mysql-server mysql-client

sudo apt-get install oracle-java8-jdk  
sudo apt-get install curl php5-cli git  
curl -sS https://getcomposer.org/installer | sudo php -- --install-dir=/usr/local/bin --filename=composer

* Das PHP Framework verwendet .htaccess Datei die normalerweise nicht aktiviert sind. Die folgenden Zeilen müssen in /etc/apache2/apache2.conf hinzugefügt werden:

<Directory /var/www/intercom/public>

Options Indexes FollowSymLinks

AllowOverride All

Require all granted

</Directory>

<Directory /var/www/management/public>

Options Indexes FollowSymLinks

AllowOverride All

Require all granted

</Directory>

* Als nächstes noch die folgenden Befehle eingeben

sudo a2enmod rewrite & sudo service apache2 restart

## Apache2 Einrichtung und SSL Zertifikate

Bevor die Webapplikationen installiert werden können, müssen zwei Virtual Host eingerichtet werden. Die Client-Webapplikation benötigt zusätzlich ein gültiges TLS-Zertifikat. (Self-Signed).

* Aktivierung von SSL in Apache

sudo a2enmod ssl

sudo service apache2 restart

* Erstellung SSL Zertifikat für die Client Webapplikation.  
  Als Hostname wird hier als Beispiel intercom.app verwendet. Zuerst muss eine Konfigurationsdatei *(v3.ext)* mit dem folgenden Inhalt generiert werden:

authorityKeyIdentifier=keyid,issuer

basicConstraints=CA:TRUE

keyUsage = digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment

subjectAltName = @alt\_names

[alt\_names]

DNS.1 = intercom.app

Falls ein IP Als hostname verwendet wird, kann man *@alt\_names* mit *IP:192.168.0.18* ersetzen.

* Nun müssen folgende Befehle eingegeben werden. Wenn gefragt, muss der Hostname als Common Name (CN) Eingegeben werden. Als Password kann immer dieselbe verwendet werden und muss das Keystore Password der Signaling-Server entsprechen.

sudo openssl genrsa -des3 -out rootCA.key 2048

sudo openssl req -x509 -new -nodes -key rootCA.key -sha256 -days 1024 -out rootCA.pem

sudo openssl req -new -sha256 -nodes -out server.csr -newkey rsa:2048 -keyout server.key

sudo openssl x509 -req -in server.csr -CA rootCA.pem -CAkey rootCA.key -CAcreateserial -out server.crt -days 500 -sha256 -extfile v3.ext

sudo openssl pkcs12 -export -in server.crt -inkey server.key -out cert.p12

sudo keytool -importkeystore -srckeystore cert.p12 -srcstoretype PKCS12 -destkeystore keystore.jks -deststoretype JKS

sudo openssl x509 -inform PEM -outform DER -in server.crt -out phone.der.crt

Somit wurden diverse Dateien generiert. Die folgenden werden später gebraucht.

* + server.cert & server.key -> SSL Zertifikate für Apache2
  + rootCA.pem -> Root CA. Das muss in den Client-Browser importiert werden, damit die Clients den Server als Vertraulich erkennen.
  + phone.der.crt -> Root CA für Mobilegeräte. Bei Mobilegeräte kann es per E-Mail verschickt werden und dann aus der Systemeinstellungen installiert werden.
  + keystore.jks -> Das muss später in die Selber Verzeichnis kopiert werden, wo der SignalingServer installiert wird.
* Erstellung von Apache2 VirtualHosts. Die zwei VirtualHosts werden die zwei Webapplikationen entsprechen (Client/Intercom App, Management Tool App). Diese werden unter verschiedene Ports lauschen. Für das müssen zwei Konfigurationsdatei unter /etc/apache2/sites-available erstellt werden.  
  Die Default-Konfiguration ist bereits vorhanden, somit können die zwei Datei wie folgendes generiert werden.

cd /etc/apache2/sites-available

sudo cp default-ssl.conf intercom.conf  
sudo cp default-ssl.conf management.conf

* In diese Dateien müssen die folgenden Zeilen angepasst werden:

…

<VirtualHost \*:443> *(\*:444)*

…

DocumentRoot /var/www/intercom/public *(/management/public)*…

SSLCertificateFile /path/to/the/cert/server.crt

SSLCertificateKeyFile /path/to/the/cert/server.key

* Nun müssen die zwei Ports noch aktiviert werden. Datei /etc/apache2/ports.conf editieren:

<IfModule ssl\_module>

Listen 443

Listen 444

</IfModule>

* Zum Abschliessen noch die folgenden Befehle eingeben:

sudo mkdir /var/www/intercom/

sudo mkdir /var/www/management/  
sudo a2ensite intercom.conf  
sudo a2ensite management.conf

sudo service apache2 reload  
sudo service apache2 restart  
sudo reboot

Jetzt sollten die zwei VirtualHosts unter die Ports 443 und 444 per SSH erreichbar sein.

## Deploy Webapplikationen

* Die beide Webapplikationen müssen zuerst auf dem Server unter den passenden Verzeichnissen kopiert werden.
  + /var/www/management
  + /var/www/intercom
* Rechte anpassen

sudo chmod -R 775 /var/www

sudo chmod -R 777 /var/www/management/storage

sudo chmod -R 775 /var/www/intercom/storage

* MySQL Database erstellen, dann Anmeldedaten und Database Name in der Datei: .env eingeben. (Falls .env nicht vorhanden: cp .env.example .env)
* Webapplikation installieren: (Diese befehle müssen in der Root Dir von jede Webapp eingegeben werden.)

composer install

php artisan migrate (Muss nur für das Management Webapp gemacht werden)

php artisan key:generate

Die zwei Webapps müssten nun aufrufbar sein.

## Deploy Dienste & Services

* Zuerst die benötigten Pfade erstellen

mkdir /home/pi/server/signalingServer

mkdir /home/pi/server/relayController

* Die beide kompilierte JARs in den entsprechenden Verzeichnissen kopieren. Die kompilierten JARs sind in den jeweilige Projekts Verzeichnisse unter /deploy zu finden.
* Nun muss noch für den SignalingServer noch das vorher hergestellte keystore.jks kopiert werden. Der Keystore muss sich in dem gleichen Verzeichnis wie der Signaling Server befinden.
* Beide Skripts müssen «Execute» Berechtigungen besitzen. (chmod +x)
* Für beide Dienste muss noch das autostart Skript unter /etc/init.d/ kopiert werden. Die Skripte sind unter dem Script-Verzeichnis gespeichert. Auch diese Skripte müssen ausführbar sein. Folgende Befehle müssen noch eingegeben werden:

sudo chmod +x /etc/init.d/signalingServer

sudo chmod +x /etc/init.d/relayController

sudo update-rc.d signalingServer defaults

sudo update-rc.d relayController

dfvd