

# Box

Setup for my personal (pet) server.

---

Felix Pojtinger

2021-12-11

# Introduction

---

**Found an error or have a suggestion?** Please open an issue on GitHub ([github.com/poijntfx/box](https://github.com/poijntfx/box)):



**Figure 1:** QR-Code to the source code on GitHub

This document and included source code is Free Culture/Free Software.



**Figure 2:** Badge of the AGPL-3.0 license

Box (c) 2021 Felix Pojtinger

SPDX-License-Identifier: AGPL-3.0

# Debian

---

# Debian

```
sudo umount /dev/mmcblk0{,p1,p0}  
curl -L 'https://raspi.debian.net/tested/20210823_r  
sudo dd if=/tmp/debian.img of=/dev/mmcblk0 bs=4M st  
sync
```

```
sudo mkdir -p /mnt/raspi-boot  
sudo mount /dev/mmcblk0p1 /mnt/raspi-boot  
{  
    echo "root_pw=$(openssl rand -base64 12)"  
    echo "root_authorized_key=$(cat ~/.ssh/id_rsa.p  
    echo "hostname=jeans-box"  
} >>/mnt/raspi-boot/sysconf.txt  
sudo umount /dev/mmcblk0{,p1,p0}
```

# IPv6

---

# IPv6

```
ssh root@jeans-box
tee /etc/sysctl.d/privacy.conf <<'EOT'
net.ipv6.conf.all.use_tempaddr=2
EOT
sysctl -p

tee /etc/network/interfaces.d/eth0 <<'EOT'
auto eth0
iface eth0 inet dhcp

iface eth0 inet6 static
    address 2001:7c7:2121:8d00::3
    autoconf 1
    accept_ra 2
EOT
```



# DNS

---

|             |       |    |      |               |
|-------------|-------|----|------|---------------|
| jeans—box   | 10800 | IN | AAAA | 2001:7c7:2121 |
| *.jeans—box | 10800 | IN | AAAA | 2001:7c7:2121 |

# SSH

---

# SSH

```
ssh root@jeans-box.example.com
apt update
apt install -y sudo curl openssh-server locales
systemctl enable --now ssh
```

```
echo "LC_ALL=en_US.UTF-8" | tee -a /etc/environment
echo "en_US.UTF-8 UTF-8" | tee /etc/locale.gen
echo "LANG=en_US.UTF-8" | tee /etc/locale.conf
locale-gen en_US.UTF-8
```

```
adduser jean
su jean -c "mkdir -m 700 -p ~/.ssh && curl 'https://
usermod -aG sudo jean
```

```
echo 'PermitRootLogin no' | tee /etc/ssh/ssh_config
```

**firewalld**

---

# firewalld

```
ssh jean@jeans-box.example.com
sudo apt update
sudo apt install -y firewalld
sudo systemctl enable --now firewalld
sudo firewall-cmd --zone=public --add-interface=eth0
sudo firewall-cmd --permanent --add-service=mdns
sudo firewall-cmd --permanent --add-service=llmnr
sudo firewall-cmd --reload
```

**APT**

---

# APT

```
ssh jean@jeans-box.example.com
sudo apt update
sudo apt install -y unattended-upgrades

sudo tee /etc/apt/apt.conf.d/50unattended-upgrades
Unattended-Upgrade::Origins-Pattern {
    "origin=*";
}
Unattended-Upgrade::Automatic-Reboot "true";
Unattended-Upgrade::Automatic-Reboot-Time "02:00";
EOT
sudo systemctl enable --now unattended-upgrades
sudo unattended-upgrades --debug
```



# Traefik

---

# Traefik

```
ssh jean@jeans-box.example.com
sudo apt update
sudo apt install -y podman
echo 'unqualified-search-registries=["docker.io"]'
sudo systemctl enable --now podman-auto-update.timer

sudo mkdir -p /etc/traefik
sudo tee /etc/traefik/traefik.yaml <<'EOT'
entryPoints:
  web:
    address: ":80"

  websecure:
    address: ":443"
```

# Cockpit

---

```
echo 'deb http://deb.debian.org/debian bullseye-backports' > /etc/apt/sources.list.d/backports.list
sudo apt update
sudo apt install -t bullseye-backports -y cockpit cockpit-pam
curl https://cockpit.jeans-box.example.com/ # Test
```

# Gitea

---

```
sudo mkdir -p /var/lib/gitea
sudo podman run -d --restart=always --label "io.com
sudo firewall-cmd --permanent --add-port=2222/tcp
sudo firewall-cmd --reload
```

```
curl https://gitea.jeans-box.example.com/ # Test Co
```

Now visit <https://gitea.jeans-box.example.com/> and run the Wizard; use the following values:

- SSH Server Domain: [gitea.jeans-box.example.com](https://gitea.jeans-box.example.com/)
- SSH Server Port: 2222
- Gitea Base URL: <https://gitea.jeans-box.example.com/>
- Use your email SMTP server in Email Settings, enable Email Notifications and Require Email Confirmation to Register

**Dex**

---

First, setup Gitea by visiting <https://gitea.jeans-box.example.com/user/settings/applications> and adding a new OAuth2 application with Application Name Dex and Redirect URI <https://dex.jeans-box.example.com/callback>. Note the client ID and client secret; we'll need them in the following.

```
sudo mkdir -p /etc/dex
sudo mkdir -p /var/lib/dex
sudo touch /var/lib/dex/dex.db
sudo chown -R 1001:1001 /var/lib/dex/
sudo tee /etc/dex/config.yaml<<'EOT'
issuer: https://dex.jeans-box.example.com

storage:
    type: sqlite3
```



**liwasc**

---

```
sudo mkdir -p /var/lib/liwasc  
sudo podman run -d --restart=always --label "io.com
```

Now visit <https://pojntfx.github.io/liwasc/> as we did before and use <wss://liwasc.jeans-box.example.com/> as the backend URL (note the trailing slash!).

**bofied**

---

# bofied

```
sudo mkdir -p /var/lib/bofied
sudo podman run -d --restart=always --label "io.com
sudo firewall-cmd --permanent --add-port=67/udp
sudo firewall-cmd --permanent --add-port=69/udp
sudo firewall-cmd --permanent --add-port=4011/udp
sudo firewall-cmd --reload
```

Now visit <https://pojntfx.github.io/bofied/> and login using the following credentials:

- Backend URL: <https://bofied.jeans-box.example.com/>
- OIDC Issuer: <https://dex.jeans-box.example.com>
- OIDC Client ID: bofied
- OIDC Redirect URL: <https://pojntfx.github.io/bofied/>