
Box

Setup for my personal (pet) server.

Felix Pojtinger

2021-12-11

Contents

1	Introduction	3
1.1	Contributing	3
1.2	License	3
2	Debian	4
3	IPv6	4
4	DNS	4
5	SSH	5
6	firewalld	5
7	APT	5
8	Traefik	6

1 Introduction

1.1 Contributing

Found an error or have a suggestion? Please open an issue on GitHub (github.com/pojntfx/box):



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

1.2 License

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

2 Debian

```
1 sudo umount /dev/mmcblk0{,p1,p0}
2 curl -L 'https://raspi.debian.net/tested/20210823_raspi_3_bullseye.img.xz' | xzcat >/tmp/debian.img
3 sudo dd if=/tmp/debian.img of=/dev/mmcblk0 bs=4M status=progress
4 sync
5
6 sudo mkdir -p /mnt/raspi-boot
7 sudo mount /dev/mmcblk0p1 /mnt/raspi-boot
8 {
9     echo "root_pw=$(openssl rand -base64 12)"
10    echo "root_authorized_key=$(cat ~/.ssh/id_rsa.pub)"
11    echo "hostname=jeans-box"
12 } >>/mnt/raspi-boot/sysconf.txt
13 sudo umount /dev/mmcblk0{,p1,p0}
```

3 IPv6

```
1 ssh root@jeans-box
2 tee /etc/sysctl.d/privacy.conf <<'EOT'
3 net.ipv6.conf.all.use_tempaddr=2
4 EOT
5 sysctl -p
6
7 tee /etc/network/interfaces.d/eth0 <<'EOT'
8 auto eth0
9 iface eth0 inet dhcp
10
11 iface eth0 inet6 static
12     address 2001:7c7:2121:8d00::3
13     autoconf 1
14     accept_ra 2
15 EOT
16 systemctl restart networking
17
18 tee /etc/resolv.conf <<'EOT'
19 nameserver 2606:4700:4700::1111
20 nameserver 2606:4700:4700::1001
21 EOT
22 sed -i /etc/hosts -e 's/\tlocalhost/\tlocalhost jeans-box/g'
```

4 DNS

1	jeans-box	10800	IN	AAAA	2001:7c7:2121:8d00::3
2	*.jeans-box	10800	IN	AAAA	2001:7c7:2121:8d00::3

5 SSH

```
1 ssh root@jeans-box.example.com
2 apt update
3 apt install -y sudo curl openssh-server
4 systemctl enable --now ssh
5
6 adduser jean
7 su jean -c "mkdir -m 700 -p ~/.ssh && curl 'https://github.com/jean.
    keys' | tee -a ~/.ssh/authorized_keys && chmod 600 ~/.ssh/
    authorized_keys"
8 usermod -aG sudo jean
9
10 echo 'PermitRootLogin no' | tee /etc/ssh/ssh_config.d/no-root.conf
11
12 passwd -d root
13 passwd -l root
14 chsh -s /sbin/nologin
15 rm ~/.ssh/authorized_keys
16
17 systemctl restart ssh
```

6 firewall

```
1 ssh jean@jeans-box.example.com
2 sudo apt update
3 sudo apt install -y firewall
4 sudo systemctl enable --now firewall
5 sudo firewall-cmd --permanent --add-service=mdns
6 sudo firewall-cmd --permanent --add-service=llmnr
```

7 APT

```
1 ssh jean@jeans-box.example.com
2 sudo apt update
3 sudo apt install -y unattended-upgrades
4
5 sudo tee /etc/apt/apt.conf.d/50unattended-upgrades <<'EOT'
6 Unattended-Upgrade::Origins-Pattern {
```

```
7   "origin=*";
8 }
9 Unattended-Upgrade::Automatic-Reboot "true";
10 Unattended-Upgrade::Automatic-Reboot-Time "02:00";
11 EOT
12 sudo systemctl enable --now unattended-upgrades
13 sudo unattended-upgrades --debug
```

8 Traefik

```
1 ssh jean@jeans-box.example.com
2 sudo apt update
3 sudo apt install -y docker.io
4 sudo systemctl enable --now docker
5
6 sudo mkdir -p /etc/traefik
7 sudo tee /etc/traefik/traefik.yaml<<'EOT'
8 entryPoints:
9   web:
10     address: ":80"
11
12   websecure:
13     address: ":443"
14
15   websecurealt:
16     address: ":8443"
17
18 providers:
19   file:
20     filename: /etc/traefik/services.yaml
21     watch: true
22
23 api:
24   dashboard: true
25
26 certificatesResolvers:
27   letsencrypt:
28     acme:
29       email: jean@example.com
30       storage: /var/lib/traefik/acme.json
31       httpChallenge:
32         entryPoint: web
33
34 log:
35   level: INFO
36 EOT
37
38 sudo tee /etc/traefik/services.yaml<<'EOT'
```

```
39 tcp:
40   routers:
41     ssh:
42       entryPoints:
43         - websecurealt
44       rule: HostSNI('*')
45       service: ssh
46     sshOverTLS:
47       entryPoints:
48         - websecure
49       rule: HostSNI('ssh.jeans-box.example.com')
50       service: ssh
51       tls:
52         certResolver: letsencrypt
53         domains:
54           - main: ssh.jeans-box.example.com
55   services:
56     ssh:
57       loadBalancer:
58         servers:
59           - address: localhost:22
60
61 http:
62   routers:
63     dashboard:
64       rule: Host('traefik.jeans-box.example.com')
65       tls:
66         certResolver: letsencrypt
67         domains:
68           - main: traefik.jeans-box.example.com
69       service: api@internal
70       entryPoints:
71         - websecure
72       middlewares:
73         - dashboard
74     cockpit:
75       rule: Host('cockpit.jeans-box.example.com')
76       tls:
77         certResolver: letsencrypt
78         domains:
79           - main: cockpit.jeans-box.example.com
80       service: cockpit
81       entryPoints:
82         - websecure
83     gitea:
84       rule: Host('gitea.jeans-box.example.com')
85       tls:
86         certResolver: letsencrypt
87         domains:
88           - main: gitea.jeans-box.example.com
89       service: gitea
```

```
90     entryPoints:
91       - websecure
92   dex:
93     rule: Host(`dex.jeans-box.example.com`)
94     tls:
95       certResolver: letsencrypt
96       domains:
97         - main: dex.jeans-box.example.com
98     service: dex
99     entryPoints:
100       - websecure
101
102   middlewares:
103     dashboard:
104       basicauth:
105         users:
106           - "jean:$apr1$dYdt8Zrl$TsEfzaedPGyjdrDk8EfRN." # htpasswd -nb
107             htpasswd -nb jean asdf
108
109   services:
110     cockpit:
111       loadBalancer:
112         serversTransport: cockpit
113         servers:
114           - url: https://localhost:9090
115     gitea:
116       loadBalancer:
117         servers:
118           - url: http://localhost:3000
119     dex:
120       loadBalancer:
121         servers:
122           - url: http://localhost:5556
123
124   serversTransports:
125     cockpit:
126       insecureSkipVerify: true
127
128   EOT
129
130   sudo docker run -d --restart=always --net=host -v /var/lib/traefik/:/
131     var/lib/traefik -v /etc/traefik/:/etc/traefik --name traefik traefik
132
133   sudo firewall-cmd --permanent --add-service=http
134   sudo firewall-cmd --permanent --add-service=https
135   sudo firewall-cmd --permanent --add-port=8443/tcp
136
137   curl -Lu jean:asdf https://traefik.jeans-box.example.com/ # Test the
138     Traefik dashboard
139
140   ssh -p 8443 pojntfx@jeans-box.example.com # Test SSH over TCP
141   ssh -o ProxyCommand="openssl s_client -connect ssh.jeans-box.example.
142     com:443 -quiet" pojntfx # Test SSH over TLS
```