
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	6
8	Traefik	6
9	Cockpit	10
10	Gitea	10
11	Dex	10
12	liwasc	12
13	bofied	12

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 chatr +i /etc/resolv.conf
23 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 locales
4 systemctl enable --now ssh
5
6 echo "LC_ALL=en_US.UTF-8" | tee -a /etc/environment
7 echo "en_US.UTF-8 UTF-8" | tee /etc/locale.gen
8 echo "LANG=en_US.UTF-8" | tee /etc/locale.conf
9 locale-gen en_US.UTF-8
10
11 adduser jean
12 su jean -c "mkdir -m 700 -p ~/.ssh && curl 'https://github.com/jean.
    keys' | tee -a ~/.ssh/authorized_keys && chmod 600 ~/.ssh/
    authorized_keys"
13 usermod -aG sudo jean
14
15 echo 'PermitRootLogin no' | tee /etc/ssh/ssh_config.d/no-root.conf
16
17 passwd -d root
18 passwd -l root
19 chsh -s /sbin/nologin
20 rm ~/.ssh/authorized_keys
21
22 systemctl restart ssh
```

6 firewalld

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

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 podman
4 echo 'unqualified-search-registries=["docker.io"]' | sudo tee /etc/
   containers/registries.conf.d/docker.conf
5 sudo systemctl enable --now podman-auto-update.timer
6
7 sudo mkdir -p /etc/traefik
8 sudo tee /etc/traefik/traefik.yaml<<'EOT'
9 entryPoints:
10     web:
11         address: ":80"
12
13     websecure:
14         address: ":443"
15
16     sshalt:
17         address: ":2222"
18
19     websecurealt:
20         address: ":8443"
21
22 providers:
23     file:
24         filename: /etc/traefik/services.yaml
25         watch: true
26
27 api:
28     dashboard: true
```

```
29
30 certificatesResolvers:
31   letsencrypt:
32     acme:
33       email: jean@example.com
34       storage: /var/lib/traefik/acme.json
35       httpChallenge:
36         entryPoint: web
37
38 log:
39   level: INFO
40 EOT
41
42 sudo tee /etc/traefik/services.yaml<<'EOT'
43 tcp:
44   routers:
45     ssh:
46       entryPoints:
47         - websecurealt
48       rule: HostSNI(`*`)
49       service: ssh
50     giteaSSH:
51       entryPoints:
52         - sshalt
53       rule: HostSNI(`*`)
54       service: giteaSSH
55     sshOverTLS:
56       entryPoints:
57         - websecure
58       rule: HostSNI(`ssh.jeans-box.example.com`)
59       service: ssh
60     tls:
61       certResolver: letsencrypt
62       domains:
63         - main: ssh.jeans-box.example.com
64   services:
65     ssh:
66       loadBalancer:
67         servers:
68           - address: localhost:22
69     giteaSSH:
70       loadBalancer:
71         servers:
72           - address: localhost:3022
73
74 http:
75   routers:
76     dashboard:
77       rule: Host(`traefik.jeans-box.example.com`)
78     tls:
79       certResolver: letsencrypt
```

```
80     domains:
81       - main: traefik.jeans-box.example.com
82     service: api@internal
83     entryPoints:
84       - websecure
85     middlewares:
86       - dashboard
87   cockpit:
88     rule: Host(`cockpit.jeans-box.example.com`)
89     tls:
90       certResolver: letsencrypt
91       domains:
92         - main: cockpit.jeans-box.example.com
93     service: cockpit
94     entryPoints:
95       - websecure
96   gitea:
97     rule: Host(`gitea.jeans-box.example.com`)
98     tls:
99       certResolver: letsencrypt
100     domains:
101       - main: gitea.jeans-box.example.com
102     service: gitea
103     entryPoints:
104       - websecure
105   dex:
106     rule: Host(`dex.jeans-box.example.com`)
107     tls:
108       certResolver: letsencrypt
109       domains:
110         - main: dex.jeans-box.example.com
111     service: dex
112     entryPoints:
113       - websecure
114   liwasc:
115     rule: Host(`liwasc.jeans-box.example.com`)
116     tls:
117       certResolver: letsencrypt
118       domains:
119         - main: liwasc.jeans-box.example.com
120     service: liwasc
121     entryPoints:
122       - websecure
123   bofied:
124     rule: Host(`bofied.jeans-box.example.com`)
125     tls:
126       certResolver: letsencrypt
127       domains:
128         - main: bofied.jeans-box.example.com
129     service: bofied
130     entryPoints:
```



```
131         - websecure
132
133     middlewares:
134         dashboard:
135             basicauth:
136                 users:
137                     - "jean:$apr1$dYdt8Zrl$TsEfzaedPGyjdrDk8EfRN." # htpasswd -nb
138                         htpasswd -nb jean asdf
139
140     services:
141         cockpit:
142             loadBalancer:
143                 serversTransport: cockpit
144                 servers:
145                     - url: https://localhost:9090
146         gitea:
147             loadBalancer:
148                 servers:
149                     - url: http://localhost:3000
150         dex:
151             loadBalancer:
152                 servers:
153                     - url: http://localhost:5556
154         liwasc:
155             loadBalancer:
156                 servers:
157                     - url: http://localhost:15124
158         bofied:
159             loadBalancer:
160                 servers:
161                     - url: http://localhost:15256
162
163     serversTransports:
164         cockpit:
165             insecureSkipVerify: true
166
167 EOT
168
169 sudo podman run -d --restart=always --net=host --label "io.containers.
170     autoupdate=image" -v /var/lib/traefik/:/var/lib/traefik -v /etc/
171     traefik/:/etc/traefik --name traefik traefik
172
173
174 sudo firewall-cmd --permanent --add-service=http
175 sudo firewall-cmd --permanent --add-service=https
176 sudo firewall-cmd --permanent --add-port=8443/tcp
177 sudo firewall-cmd --reload
178
179 curl -Lu jean:asdf https://traefik.jeans-box.example.com/ # Test the
180     Traefik dashboard
181
182 ssh -p 8443 jean@jeans-box.example.com # Test SSH over TCP
183
184 ssh -o ProxyCommand="openssl s_client -connect ssh.jeans-box.example.
185     com:443 -quiet" jean # Test SSH over TLS
```

9 Cockpit

```
1 echo 'deb http://deb.debian.org/debian bullseye-backports main' | sudo
  tee /etc/apt/sources.list.d/backports.list
2 sudo apt update
3 sudo apt install -t bullseye-backports -y cockpit cockpit-podman
  cockpit-pcp
4
5 curl https://cockpit.jeans-box.example.com/ # Test Cockpit
```

10 Gitea

```
1 sudo mkdir -p /var/lib/gitea
2 sudo podman run -d --restart=always --label "io.containers.autoupdate=
  image" --net slirp4netns:allow_host_loopback=true,enable_ipv6=true -
  p 3000:3000 -p 3022:22 -v /var/lib/gitea:/data -v /etc/timezone:/
  etc/timezone:ro -v /etc/localtime:/etc/localtime:ro -e 'USER_UID
  =1000' -e 'USER_GID=1000' --name gitea gitea/gitea
3 sudo firewall-cmd --permanent --add-port=2222/tcp
4 sudo firewall-cmd --reload
5
6 curl https://gitea.jeans-box.example.com/ # Test Cockpit
```

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

- SSH Server Domain: `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`
- Under `Server` and `Third-Party Service Settings`, enable `Disable Self-Registration` (if you want to prevent others from using Gitea)
- Under `Administrator Account Settings`, create your admin account

Note that the installation might take a while (about 1 minute)

11 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.

```
1 sudo mkdir -p /etc/dex
2 sudo mkdir -p /var/lib/dex
3 sudo touch /var/lib/dex/dex.db
4 sudo chown -R 1001:1001 /var/lib/dex/
5 sudo tee /etc/dex/config.yaml<<'EOT'
6 issuer: https://dex.jeans-box.example.com
7
8 storage:
9   type: sqlite3
10  config:
11    file: /var/dex/dex.db
12
13 web:
14   http: 0.0.0.0:5556
15   allowedOrigins: ['*']
16
17 staticClients:
18   - id: liwasc
19     redirectURIs:
20       - https://pojntfx.github.io/liwasc/
21     name: "liwasc"
22     public: true
23   - id: bofied
24     redirectURIs:
25       - https://pojntfx.github.io/bofied/
26     name: "bofied"
27     public: true
28
29 connectors:
30   - type: gitea
31     id: gitea
32     name: Gitea
33     config:
34       clientID: yourclientidfromgiteahere
35       clientSecret: yourclientsecretfromgiteahere
36       redirectURI: https://dex.jeans-box.example.com/callback
37       baseURL: https://gitea.jeans-box.example.com
38 EOT
39 sudo podman run -d --restart=always --label "io.containers.autoupdate=
  image" --net slirp4netns:allow_host_loopback=true,enable_ipv6=true -
  p 5556:5556 -v /var/lib/dex:/var/dex -v /etc/dex:/etc/dex --name dex
  ghcr.io/dexidp/dex dex serve /etc/dex/config.yaml
```

You can test it out by visiting <https://pojntfx.github.io/liwasc/> and trying to log in using the following credentials:

- Backend URL: `ws://example.com/` (we'll set this later; this is just to try out the login)

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

And authorization prompt from Gitea and Dex should show up, after which liwasc's home page should load (showing an error like `Failed to construct 'WebSocket': An insecure WebSocket connection may not be initiated from a page loaded over HTTPS.`).

12 liwasc

```
1 sudo mkdir -p /var/lib/liwasc
2 sudo podman run -d --restart=always --label "io.containers.autoupdate=
  image" --net host --cap-add NET_RAW --ulimit nofile=16384:16384 -v /
  var/lib/liwasc:/root/.local/share/liwasc -e
  LIWASC_BACKEND_OIDCISSUER=https://dex.jeans-box.example.com -e
  LIWASC_BACKEND_OIDCLIENTID=liwasc -e LIWASC_BACKEND_DEVICENAME=eth0
  -e LIWASC_BACKEND_PERIODICSCANCRONEXPRESSION='0 0 * * *' --name
  liwasc pojntfx/liwasc-backend
```

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!).

13 bofied

```
1 sudo mkdir -p /var/lib/bofied
2 sudo podman run -d --restart=always --label "io.containers.autoupdate=
  image" --net host --cap-add NET_BIND_SERVICE -v /var/lib/bofied:/
  root/.local/share/bofied -e BOFIED_BACKEND_OIDCISSUER=https://dex.
  felicias-box.alphahorizon.io -e BOFIED_BACKEND_OIDCLIENTID=bofied -
  e BOFIED_BACKEND_ADVERTISEDIP=100.64.154.249 --name bofied pojntfx/
  bofied-backend
3 sudo firewall-cmd --permanent --add-port=67/udp
4 sudo firewall-cmd --permanent --add-port=69/udp
5 sudo firewall-cmd --permanent --add-port=4011/udp
6 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/>