Box

Setup for my personal (pet) server.

Felix Pojtinger

2021-12-11

Contents

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

```
sudo umount /dev/mmcblk0{,p1,p0}
curl -L 'https://raspi.debian.net/tested/20210823_raspi_3_bullseye.img.xz' | xzcat >/tmp/debian.img
sudo dd if=/tmp/debian.img of=/dev/mmcblk0 bs=4M status=progress
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.pub)"
    echo "hostname=jeans-box"
} >>/mnt/raspi-boot/sysconf.txt
sudo umount /dev/mmcblk0{,p1,p0}
```

3 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
systemctl restart networking

tee /etc/resolv.conf <<'EOT'
nameserver 2606:4700:4700::1111
nameserver 2606:4700:4700::1001
EOT
sed -i /etc/hosts -e 's/\tlocalhost/\tlocalhost jeans-box/g'
```

4 DNS

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

5 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://github.com/jean.
    keys' | tee -a ~/.ssh/authorized_keys && chmod 600 ~/.ssh/
    authorized_keys"
usermod -aG sudo jean

echo 'PermitRootLogin no' | tee /etc/ssh/ssh_config.d/no-root.conf

passwd -d root
passwd -l root
chsh -s /sbin/nologin
rm ~/.ssh/authorized_keys

systemctl restart ssh
```

6 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 --permanent
sudo firewall-cmd --permanent --add-service=mdns
sudo firewall-cmd --permanent --add-service=llmnr
sudo firewall-cmd --reload
```

7 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 <<'EOT'
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
```

8 Traefik

```
ssh jean@jeans-box.example.com
sudo apt update
sudo apt install -y podman
echo 'unqualified-search-registries=["docker.io"]' | sudo tee /etc/containers/registries.conf.d/docker.conf

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

  websecure:
    address: ":443"

  websecurealt:
    address: ":8443"

providers:
  file:
    filename: /etc/traefik/services.yaml
    watch: true

api:
  dashboard: true

certificatesResolvers:
  letsencrypt:
    acme:
      email: jean@example.com
      storage: /var/lib/traefik/acme.json
      httpChallenge:
        entryPoint: web

log:
  level: INFO
EOT

sudo tee /etc/traefik/services.yaml<<'EOT'
tcp:
  routers:
    ssh:
      entryPoints:
        - websecurealt
      rule: HostSNI(`*`)
      service: ssh
    sshOverTLS:
      entryPoints:
        - websecure
      rule: HostSNI(`ssh.jeans-box.example.com`)
      service: ssh
      tls:
        certResolver: letsencrypt
        domains:
          - main: ssh.jeans-box.example.com
  services:
    ssh:
      loadBalancer:
        servers:
          - address: localhost:22

http:
  routers:
    dashboard:
      rule: Host(`traefik.jeans-box.example.com`)
      tls:
        certResolver: letsencrypt
        domains:
          - main: traefik.jeans-box.example.com
      service: api@internal
      entryPoints:
        - websecure
      middlewares:
        - dashboard
    cockpit:
      rule: Host(`cockpit.jeans-box.example.com`)
      tls:
        certResolver: letsencrypt
        domains:
          - main: cockpit.jeans-box.example.com
      service: cockpit
      entryPoints:
        - websecure
    gitea:
      rule: Host(`gitea.jeans-box.example.com`)
      tls:
        certResolver: letsencrypt
        domains:
          - main: gitea.jeans-box.example.com
      service: gitea
      entryPoints:
        - websecure
    dex:
      rule: Host(`dex.jeans-box.example.com`)
      tls:
        certResolver: letsencrypt
        domains:
          - main: dex.jeans-box.example.com
      service: dex
      entryPoints:
        - websecure

  middlewares:
    dashboard:
      basicauth:
        users:
          - "jean:$apr1$dYdt8Zrl$TsEfzaedPGyjdrDk8EfRN." # htpasswd -nb htpasswd -nb jean asdf

  services:
    cockpit:
      loadBalancer:
        serversTransport: cockpit
        servers:
          - url: https://localhost:9090
    gitea:
      loadBalancer:
        servers:
          - url: http://localhost:3000
    dex:
      loadBalancer:
        servers:
          - url: http://localhost:5556

  serversTransports:
    cockpit:
      insecureSkipVerify: true
EOT

sudo podman run -d --restart=always --net=host -v /var/lib/traefik/:/var/lib/traefik -v /etc/traefik/:/etc/traefik --name traefik traefik

sudo firewall-cmd --permanent --add-service=http
sudo firewall-cmd --permanent --add-service=https
sudo firewall-cmd --permanent --add-port=8443/tcp
sudo firewall-cmd --reload

curl -Lu jean:asdf https://traefik.jeans-box.example.com/ # Test the Traefik dashboard
ssh -p 8443 pojntfx@jeans-box.example.com # Test SSH over TCP
ssh -o ProxyCommand="openssl s_client -connect ssh.jeans-box.example.com:443 -quiet" pojntfx # Test SSH over TLS
```

9 Cockpit

```
echo 'deb http://deb.debian.org/debian bullseye-backports main' | sudo tee /etc/apt/sources.list.d/backports.list
sudo apt update
sudo apt install -t bullseye-backports -y cockpit cockpit-podman

curl https://cockpit.jeans-box.example.com/ # Test Cockpit
```