#### Uni Software Defined Infrastructure Notes

Felix Pojtinger

December 20, 2021

```
IIILIOUUCLIOII
   Contributing
   License
Hosts
User
SSH
UFW
APT
Traefik
Cockpit
DNS
   Manager
   Worker
   Exercises
LDAP
Apache
```





#### Contributing

These study materials are heavily based on professor Goik's "Software Defined Infrastructure" lecture at HdM Stuttgart.

**Found an error or have a suggestion?** Please open an issue on GitHub (github.com/pojntfx/uni-sdi-notes):



Figure 1: QR code to source repository

If you like the study materials, a GitHub star is always appreciated :)



#### License



Figure 2: AGPL-3.0 license badge

Uni Software Defined Infrastructure Notes (c) 2021 Felix Pojtinger and contributors

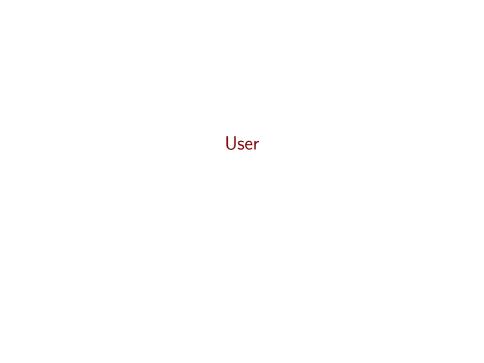
SPDX-License-Identifier: AGPL-3.0



#### Hosts

Add the following A and AAAA records to a public DNS server (with root domain alphahorizon.io):

felixs-sdi1	10800	IN	Α	138.68.70.72
felixs-sdi1	10800	IN	AAAA	2a03:b0c0:3:d0::e34
*.felixs-sdi1	10800	IN	Α	138.68.70.72
*.felixs-sdi1	10800	IN	AAAA	2a03:b0c0:3:d0::e34
felixs-sdi2	10800	IN	Α	159.223.25.154
felixs-sdi2	10800	IN	AAAA	2a03:b0c0:3:d0::109
*.felixs-sdi2	10800	IN	Α	159.223.25.154
*.felixs-sdi2	10800	IN	AAAA	2a03:b0c0:3:d0::109



#### User

ssh root@felixs-sdi1.alphahorizon.io
adduser pojntfx
usermod -aG sudo pojntfx
su pojntfx



#### SSH

```
sudo apt update
sudo apt install -y openssh-server
sudo systemctl enable --now ssh
mkdir -p ~/.ssh
chmod 700 ~/.ssh
curl 'https://github.com/pojntfx.keys' | tee -a ~/.ssh/autl
chmod 600 ~/.ssh/authorized_keys
exit
```



#### **UFW**

ssh pojntfx@felixs-sdi1.alphahorizon.io sudo apt update sudo apt install -y ufw sudo systemctl enable --now ufw sudo ufw default deny incoming sudo ufw default allow outgoing sudo ufw allow OpenSSH sudo ufw enable



#### **APT**

```
sudo apt update
sudo apt install -y unattended-upgrades
sudo vi /etc/apt/apt.conf.d/50unattended-upgrades # Now rep
Unattended-Upgrade::Origins-Pattern {
  "origin=*";
Unattended-Upgrade::Automatic-Reboot "true";
Unattended-Upgrade::Automatic-Reboot-Time "02:00";
sudo dpkg-reconfigure unattended-upgrades # Answer with yes
sudo systemctl enable --now unattended-upgrades
sudo unattended-upgrades --debug # Test the configuration;
sudo reboot # If required
```

# Traefik

#### Traefik

```
$ sudo apt update
$ sudo apt install -y docker.io
$ sudo systemctl enable --now docker
$ sudo mkdir -p /etc/traefik
$ sudo tee /etc/traefik/traefik.yaml<<'EOT'</pre>
entryPoints:
  dnsTcp:
    address: ":53"
  dnsUdp:
    address: ":53/udp"
  web:
    address: ":80"
  websecure:
    address: ":443"
```



#### Cockpit

```
echo 'deb http://deb.debian.org/debian bullseye-backports sudo apt update sudo apt install -t bullseye-backports -y cockpit
```

sudo sed -i /lib/systemd/system/cockpit.socket -e 's/Lister
sudo systemctl daemon-reload



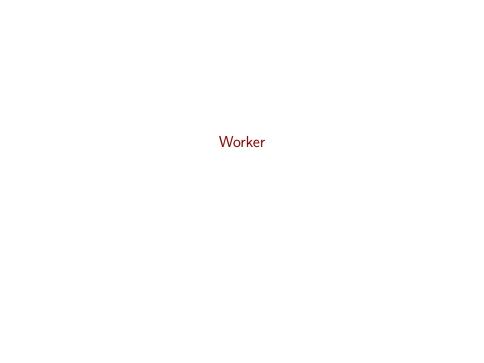


## Manager

sudo apt update

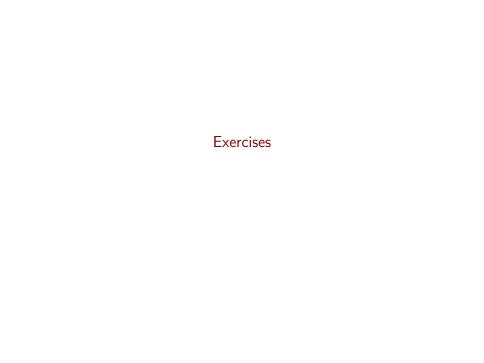
```
sudo systemctl enable --now named
sudo vi /etc/bind/named.conf.options # Now add the following
listen-on port 54 { 127.0.0.1; };
listen-on-v6 port 54 { ::1; };
version "not currently available";
recursion yes;
querylog yes;
allow-transfer { none; };
allow-query { any; };
sudo tee -a /etc/bind/named.conf.local <<'EOT'</pre>
zone "example.pojtinger" {
        type master;
        file "/etc/bind/db.example.pojtinger";
```

sudo apt install -y bind9 bind9utils



#### Worker

```
sudo apt update
sudo apt install -y bind9 bind9utils
sudo systemctl enable --now named
sudo vi /etc/bind/named.conf.options # Now add the following
listen-on port 54 { 127.0.0.1; };
listen-on-v6 port 54 { ::1; };
version "not currently available";
recursion yes;
querylog yes;
allow-transfer { none; };
allow-query { any; };
sudo tee -a /etc/bind/named.conf.local <<'EOT'</pre>
zone "example.pojtinger" {
        type slave;
        file "db.example.pojtinger";
```



#### Exercises

Use the dig command to query A/CNAME/MX/NS records from various machines/domains of your choice. Then

```
execute reverse lookups as well.
# Get A/AAA records from manager server
$ dig +noall +answer @138.68.70.72 example.pojtinger A
```

example.pojtinger. 3600 IN A 138.68.70.

\$ dig +noall +answer @138.68.70.72 example.pojtinger AAAA example.pojtinger. 3600 IN AAAA 2a03:b0c0:

```
# Get A/AAAA records from worker server
```

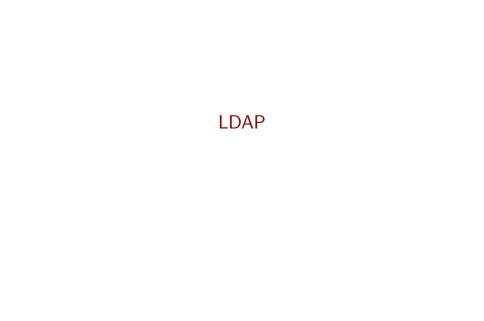
avamnla noitingar

```
$ dig +noall +answer @159.223.25.154 example.pojtinger A
example.pojtinger.
                                           138.68.70.
                     3600
                            IN
                                    Α
$ dig +noall +answer @159.223.25.154 example.pojtinger AAA
example.pojtinger.
                                    AAAA 2a03:b0c0:
```

```
# Get NS record
$ dig +noall +answer @159.223.25.154 example.pojtinger NS
```

3600 IN

3600 IN NG ng1 ayamnl



#### **LDAP**

sudo apt update
sudo apt install -y slapd ldap-utils certbot

sudo dpkg-reconfigure slapd # ldap.felixs-sdi1.alphahorizon
curl ldaps://ldap.felixs-sdi1.alphahorizon.io:443 # Test tl

socat tcp-listen:8389,fork openss1:ldap.felixs-sdi1.alphahe
curl ldap://localhost:8389 # Test the proxy's connection

# Connect in Apache Directory Studio with the following in:
# Hostname: localhost
# Port: 8389

# Bind DN or user: cn=admin,dc=ldap,dc=felixs-sdi1,dc=alpha
# Bind password: The password from `sudo dpkg-reconfigure a

# Bind password: The password from sudo dpkg-reconfigure s

# Connect with ldapwhoami like so:
ldapwhoami -H 'ldaps://ldap.felixs-sdi1.alphahorizon.io:44

Apache

#### **Apache**

sudo apt update sudo apt install -y apache2 sudo vi /etc/apache2/ports.conf # Now replace/add the follo Listen 8080 sudo systemctl restart apache2 sudo systemctl enable --now apache2

sudo systemctl status apache2 sudo tree -T "Example Index" -H '.' -o /var/www/html/index

sudo mkdir -p /var/www/sdidoc sudo tree -T "Example Index For sdidoc" -H '.' -o /var/www, sudo tee /etc/apache2/sites-available/apache.felixs-sdi1.a

<VirtualHost \*:8080> ServerName felixs-sdi1.alphahorizon.io

ServerAdmin webmaster@alphahorizon.io

DocumentRoot /var/www/html

ServerAlias apache.felixs-sdi1.alphahorizon.io



# MariaDB and phpMyAdmin

sudo apt update
sudo apt install -y mariadb-server
sudo mysql\_secure\_installation # Empty string, y, y, yourpa
sudo mysql -u root -e 'GRANT ALL PRIVILEGES ON \*.\* TO 'phpr

sudo apt install -y phpmyadmin libapache2-mod-php # apache

sudo a2disconf phpmyadmin

sudo phpenmod mbstring

sudo tee /etc/apache2/sites-available/phpmyadmin.felixs-sd

ServerAdmin webmaster@alphahorizon.io DocumentRoot /usr/share/phpmyadmin

# LDAP Account Manager

### LDAP Account Manager

sudo apt update sudo apt install -y ldap-account-manager

sudo a2disconf ldap-account-manager

sudo tee /etc/apache2/sites-available/ldap-account-manager <VirtualHost \*:8080>

ServerName felixs-sdi1.alphahorizon.io ServerAlias ldap-account-manager.felixs-sdi1.alphal

ServerAdmin webmaster@alphahorizon.io DocumentRoot /usr/share/ldap-account-manager

> ErrorLog \${APACHE\_LOG\_DIR}/error.log CustomLog \${APACHE\_LOG\_DIR}/access.log combined

<Directory "/usr/share/ldap-account-manager"> Options +FollowSymLinks

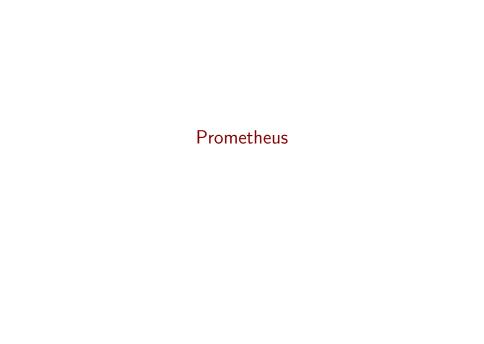


#### Nextcloud

sudo apt update

sudo mysql -u root -e "CREATE USER 'nextcloud'@'localhost' sudo mysql -u root -e "CREATE DATABASE nextcloud;" sudo mysql -u root -e "GRANT ALL PRIVILEGES ON nextcloud.\* sudo mysql -u root -e "FLUSH PRIVILEGES;" sudo tee /etc/php/\*/apache2/php.ini <<'EOT'</pre> date.timezone = Europe/Berlin memory limit = 1024M upload\_max\_filesize = 1024M post\_max\_size = 1024M max\_execution\_time = 300 EOT curl -Lo /tmp/nextcloud.zip https://download.nextcloud.com/ unzip /tmp/nextcloud.zip 'nextcloud/\*' -d /tmp/nextcloud

sudo apt install -y libapache2-mod-php php-ctype php-curl



#### **Prometheus**

```
sudo apt update
sudo apt install -y prometheus
sudo systemctl enable --now prometheus
```



#### Grafana

sudo apt update sudo apt install -y apt-transport-https software-properties curl -L https://packages.grafana.com/gpg.key | sudo apt-key echo 'deb https://packages.grafana.com/oss/deb stable main sudo apt update sudo apt install -y grafana sudo systemctl enable --now grafana-server sudo vi /etc/grafana/grafana.ini

# Replace the `[auth.ldap]` block with the following:

[auth.ldap]
enabled = true
config\_file = /etc/grafana/ldap.toml
allow\_sign\_up = true
# Replace the `[log]` block with the following: