Uni Software Defined Infrastructure Notes

Felix Pojtinger

November 8, 2021

```
Contributing
   License
Hosts
User
SSH
UFW
APT
Cockpit
Caddy
DNS
   Manager
   Worker
   Exercises
LDAP
Uni Software Defined Infrastructure Notes
```





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

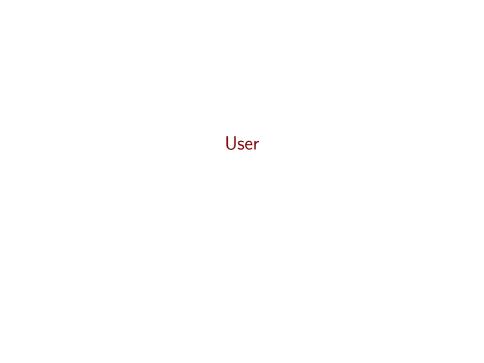
SPDX-License-Identifier: AGPL-3.0



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
```



Cockpit

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



Caddy {

```
curl -L 'https://dl.cloudsmith.io/public/caddy/stable/gpg.]
curl -L 'https://dl.cloudsmith.io/public/caddy/stable/debia
sudo apt update
sudo apt install -y caddy
sudo tee /etc/caddy/Caddyfile <<EOT</pre>
        email felix@pojtinger.com
}
cockpit.felixs-sdi1.alphahorizon.io {
        reverse proxy https://localhost:9090 {
            transport http {
                tls_insecure_skip_verify
ldap.felixs-sdi1.alphahorizon.io {
```



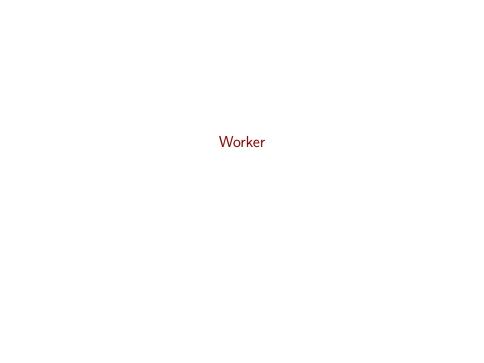


Manager sudo a sudo a

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
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" {
```

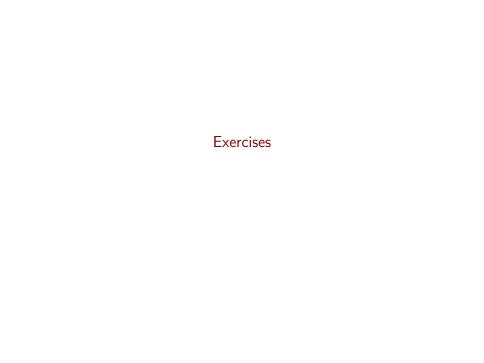
zone "example.pojtinger" {
 type master;
 file "/etc/bind/db.example.pojtinger";
 allow-query { any; };
 allow-transfer { 159.223.25.154; 2a03:b0c0:3:d0::10};



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
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";
        allow-query { any; };
        masters { 138.68.70.72; 2a03:b0c0:3:d0::e34:5001; ]
};
```



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

3600

IN

AAAA 2a03:b0c0:

AAAA 2a03:b0c0:

example.pojtinger.

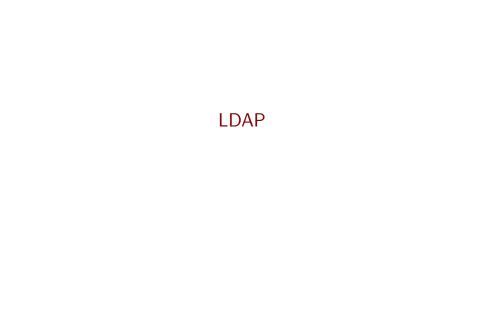
```
# Get A/AAAA records from worker server
$ dig +noall +answer @159.223.25.154 example.pojtinger A
```

example.pojtinger. 138.68.70. 3600 IN Α \$ dig +noall +answer @159.223.25.154 example.pojtinger AAA

example.pojtinger.

Get NS record \$ dig +noall +answer @159.223.25.154 example.pojtinger NS avamnla noitingar 3600 IN NG ng1 ayamnl

3600 IN



LDAP

```
sudo apt update
sudo apt install -y slapd ldap-utils certbot
sudo dpkg-reconfigure slapd # ldap.felixs-sdi1.alphahorizon
sudo ufw allow 'LDAPS' # TODO: Setup certbot
export CERT LOCATION="$(sudo bash -c 'find /var/lib/caddy/
export KEY_LOCATION="$(sudo bash -c 'find /var/lib/caddy/...
sudo mkdir -p /etc/openldap
sudo tee -a /etc/openldap/slapd.conf <<EOT</pre>
# TODO: Chown/ln and use CERT LOCATION and KEY LOCATION for
EOT
```