Uni Software Defined Infrastructure Notes

Felix Pojtinger

November 15, 2021

Uni Software Defined Infrastructure Notes

Introduction

Contributing

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

License

Figure 2: AGPL-3.0 license badge

SPDX-License-Identifier: AGPL-3.0

Hosts

Hosts

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

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

User

User

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

SSH

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/auth
chmod 600 ~/.ssh/authorized_keys
exit
```

UFW

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

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'
entryPoints:
  web:
    address: ":80"

  websecure:
    address: ":443"

  websecurealt:
    address: ":8443"

providers:
  file:
    filename: /etc/traefik/services.yaml
```

Cockpit

Cockpit

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

DNS

Manager

Manager

```
sudo apt update
sudo apt install -y bind9 bind9utils
sudo systemctl enable --now named

sudo vi /etc/bind/named.conf.options # Now add the followi
version "not currently available";
recursion yes;
querylog yes;
allow-transfer { none; };
allow-query { any; };

sudo tee -a /etc/bind/named.conf.local <<EOT
zone "example.pojtinger" {
        type master;
        file "/etc/bind/db.example.pojtinger";
        allow-query { any; };
        allow-transfer { 159.223.25.154; 2a03:b0c0:3:d0::1
};
```

Worker

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 followi
version "not currently available";
recursion yes;
querylog yes;
allow-transfer { none; };
allow-query { any; };

sudo tee -a /etc/bind/named.conf.local <<EOT
zone "example.pojtinger" {
        type slave;
        file "db.example.pojtinger";
        allow-query { any; };
        masters { 138.68.70.72; 2a03:b0c0:3:d0::e34:5001; }
};
```

Exercises

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       138.68.70.7
$ dig +noall +answer @138.68.70.72 example.pojtinger AAAA
example.pojtinger.      3600    IN      AAAA    2a03:b0c0:3

# Get A/AAAA records from worker server
$ dig +noall +answer @159.223.25.154 example.pojtinger A
example.pojtinger.      3600    IN      A       138.68.70.7
$ dig +noall +answer @159.223.25.154 example.pojtinger AAAA
example.pojtinger.      3600    IN      AAAA    2a03:b0c0:3

# Get NS record
$ dig +noall +answer @159.223.25.154 example.pojtinger NS
example.pojtinger.      3600    IN      NS      ns1.example
```

LDAP

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/.l

sudo mkdir -p /etc/openldap
sudo tee -a /etc/openldap/slapd.conf <<EOT
# TODO: Chown/ln and use CERT_LOCATION and KEY_LOCATION for
EOT
```