Uni Software Defined Infrastructure Notes

Notes for the software defined infrastructure course at HdM Stuttgart

---

Jakob Waibel Felix Pojtinger

2022-01-10

Introduction

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

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	138.68.70.7
felixs-sdi1	10800	IN	AAAA	2a03:b0c0:3
*.felixs-sdi1	10800	IN	A	138.68.70.7
*.felixs-sdi1	10800	IN	AAAA	2a03:b0c0:3
felixs-sdi2	10800	IN	A	159.223.25.
felixs-sdi2	10800	IN	AAAA	2a03:b0c0:3
*.felixs-sdi2	10800	IN	A	159.223.25.
*.felixs-sdi2	10800	IN	AAAA	2a03:b0c0:3

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 ~/.
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 #
Unattended-Upgrade::Origins-Pattern {
  "origin=*";
}
Unattended-Upgrade::Automatic-Reboot "true";
Unattended-Upgrade::Automatic-Reboot-Time "02:00";

sudo dpkg-reconfigure unattended-upgrades # Answer
sudo systemctl enable --now unattended-upgrades
sudo unattended-upgrades --debug # Test the configu
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:
  dnsTcp:
    address: ":53"

  dnsUdp:
    address: ":53/udp"

  web:
    address: ":80"

  ...
```

Cockpit

Cockpit

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

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

DNS

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
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'
```

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
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'
```

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.pojtinge
example.pojtinger.      3600    IN      A
138.68.70.72
$ dig +noall +answer @138.68.70.72 example.pojtinge
example.pojtinger.      3600    IN      AAAA
2a03:b0c0:3:d0::e34:5001

# Get A/AAAA records from worker server
$ dig +noall +answer @159.223.25.154 example.pojtin
example.pojtinger.      3600    IN      A
138.68.70.72
```

LDAP

LDAP

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

sudo dpkg-reconfigure slapd # ldap.felixs-sdi1.alph

curl ldaps://ldap.felixs-sdi1.alphahorizon.io:443 #

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

# Connect in Apache Directory Studio with the follow
# Hostname: localhost
# Port: 8389
# Bind DN or user: cn=admin,dc=ldap,dc=felixs-sdi1,
# Bind password: The password from `sudo dpkg-recon
```

Apache

Apache

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

sudo tree -T "Example Index" -H '.' -o /var/www/htm
sudo mkdir -p /var/www/sdidoc
sudo tree -T "Example Index For sdidoc" -H '.' -o /
sudo tee /etc/apache2/sites-available/apache.felixs
<VirtualHost *:8080>
        ServerName felixs-sdi1.alphahorizon.io
        ServerAlias apache.felixs-sdi1.alphahorizon
```

MariaDB and phpMyAdmin

MariaDB and phpMyAdmin

```
sudo apt update
sudo apt install -y mariadb-server
sudo mysql_secure_installation # Empty string, y, y

sudo mysql -u root -e 'GRANT ALL PRIVILEGES ON *.* T

sudo apt install -y phpmyadmin libapache2-mod-php #
sudo phpenmod mbstring

sudo a2disconf phpmyadmin

sudo tee /etc/apache2/sites-available/phpmyadmin.fe
<VirtualHost *:8080>
        ServerName felixs-sdi1.alphahorizon.io
        ServerAlias phpmyadmin.felixs-sdi1.alphahor
```

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-
<VirtualHost *:8080>
        ServerName felixs-sdi1.alphahorizon.io
        ServerAlias ldap-account-manager.felixs-sdi

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

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log com
```

Nextcloud

Nextcloud

```
sudo apt update
sudo apt install -y libapache2-mod-php php-ctype ph

sudo mysql -u root -e "CREATE USER 'nextcloud'@'loc
sudo mysql -u root -e "CREATE DATABASE nextcloud;"
sudo mysql -u root -e "GRANT ALL PRIVILEGES ON next
sudo mysql -u root -e "FLUSH PRIVILEGES;"

sudo tee /etc/php/*/apache2/php.ini <<'EOT'
date.timezone = Europe/Berlin
memory_limit = 1024M
upload_max_filesize = 1024M
post_max_size = 1024M
max_execution_time = 300
EOT
```

Prometheus

Prometheus

```
sudo apt update
sudo apt install -y prometheus

sudo systemctl enable --now prometheus

sudo tee /etc/prometheus/prometheus.yml <<'EOT'
global:
  scrape_interval:     15s
  evaluation_interval: 15s
  external_labels:
      monitor: 'example'

alerting:
  alertmanagers:
  - static_configs:
```

Grafana

Grafana

```
sudo apt update
sudo apt install -y apt-transport-https software-pr

curl -L https://packages.grafana.com/gpg.key | sudo
echo 'deb https://packages.grafana.com/oss/deb stab

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 followin
[auth.ldap]
enabled = true
```