

Uni Software Defined Infrastructure Notes

Felix Pojtinger

December 20, 2021

Contents

1 Introduction	3
1.1 Contributing	3
1.2 License	3
2 Hosts	4
3 User	4
4 SSH	4
5 UFW	4
6 APT	5
7 Traefik	5
8 Cockpit	9
9 DNS	10
9.1 Manager	10
9.2 Worker	12
9.3 Exercises	13
10 LDAP	14
11 Apache	18
12 MariaDB and phpMyAdmin	21
13 LDAP Account Manager	22
14 Nextcloud	24
15 Prometheus	25

1 Introduction

1.1 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 :)

1.2 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

2 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::e34:5001
*.felixs-sdi1	10800	IN	A	138.68.70.72
*.felixs-sdi1	10800	IN	AAAA	2a03:b0c0:3:d0::e34:5001
felixs-sdi2	10800	IN	A	159.223.25.154
felixs-sdi2	10800	IN	AAAA	2a03:b0c0:3:d0::1092:b001
*.felixs-sdi2	10800	IN	A	159.223.25.154
*.felixs-sdi2	10800	IN	AAAA	2a03:b0c0:3:d0::1092:b001

3 User

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

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

5 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
```

6 APT

```
sudo apt update
sudo apt install -y unattended-upgrades

sudo vi /etc/apt/apt.conf.d/50unattended-upgrades # Now replace/add the following:
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; this will install the available u
sudo reboot # If required
```

7 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"

  websecure:
    address: ":443"

  websecurealt:
    address: ":8443"

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

```

api:
  dashboard: true

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

log:
  level: INFO
EOT
$ sudo tee /etc/traefik/services.yaml<<'EOT'
udp:
  routers:
    dns:
      entryPoints:
        - dnsUdp
      service: dns
  services:
    dns:
      loadBalancer:
        servers:
          - address: localhost:54

tcp:
  routers:
    dns:
      entryPoints:
        - dnsTcp
      rule: HostSNI(`*`)
      service: dns
    ssh:
      entryPoints:
        - websecurealt
      rule: HostSNI(`*`)
      service: ssh
    sshOverTLS:
      entryPoints:
        - websecure
      rule: HostSNI(`ssh.felixs-sdi1.alphahorizon.io`)
      service: ssh
  tls:
    certResolver: letsencrypt

```

```

        domains:
          - main: ssh.felixs-sdi1.alphahorizon.io
ldap:
  entryPoints:
    - websecure
  rule: HostSNI(`ldap.felixs-sdi1.alphahorizon.io`)
  service: ldap
  tls:
    certResolver: letsencrypt
    domains:
      - main: ldap.felixs-sdi1.alphahorizon.io
services:
  dns:
    loadBalancer:
      servers:
        - address: localhost:54
  ssh:
    loadBalancer:
      servers:
        - address: localhost:22
  ldap:
    loadBalancer:
      servers:
        - address: localhost:389

http:
  routers:
    cockpit:
      rule: Host(`cockpit.felixs-sdi1.alphahorizon.io`)
      tls:
        certResolver: letsencrypt
        domains:
          - main: cockpit.felixs-sdi1.alphahorizon.io
      service: cockpit
      entryPoints:
        - websecure
  apache:
    rule: Host(`apache.felixs-sdi1.alphahorizon.io`) || HostRegexp(`{subdomain:[a-z]+}.alpha`)
    tls:
      certResolver: letsencrypt
      domains:
        - main: apache.felixs-sdi1.alphahorizon.io
        - main: marx.apache.felixs-sdi1.alphahorizon.io
        - main: kropotkin.apache.felixs-sdi1.alphahorizon.io
        - main: secure.apache.felixs-sdi1.alphahorizon.io
    service: apache

```

```

    entryPoints:
      - websecure
phpmyadmin:
  rule: Host(`phpmyadmin.felixs-sdi1.alphahorizon.io`)
  tls:
    certResolver: letsencrypt
    domains:
      - main: phpmyadmin.felixs-sdi1.alphahorizon.io
  service: apache
  entryPoints:
    - websecure
ldapAccountManager:
  rule: Host(`ldap-account-manager.felixs-sdi1.alphahorizon.io`)
  tls:
    certResolver: letsencrypt
    domains:
      - main: ldap-account-manager.felixs-sdi1.alphahorizon.io
  service: apache
  entryPoints:
    - websecure
nextcloud:
  rule: Host(`nextcloud.felixs-sdi1.alphahorizon.io`)
  tls:
    certResolver: letsencrypt
    domains:
      - main: nextcloud.felixs-sdi1.alphahorizon.io
  service: apache
  entryPoints:
    - websecure
grafana:
  rule: Host(`grafana.felixs-sdi1.alphahorizon.io`)
  tls:
    certResolver: letsencrypt
    domains:
      - main: grafana.felixs-sdi1.alphahorizon.io
  service: grafana
  entryPoints:
    - websecure
dashboard:
  rule: Host(`traefik.felixs-sdi1.alphahorizon.io`)
  tls:
    certResolver: letsencrypt
    domains:
      - main: traefik.felixs-sdi1.alphahorizon.io
  service: api@internal
  entryPoints:

```



```

        - websecure
    middlewares:
        - dashboard

middlewares:
    dashboard:
        basicauth:
            users:
                - "admin:$apr1$wBh8VM6G$bhz82XpyH3mX4ha9XBbcL1" # httpasswd -nb admin asdf

services:
    cockpit:
        loadBalancer:
            serversTransport: cockpit
            servers:
                - url: https://localhost:9091
    apache:
        loadBalancer:
            servers:
                - url: http://localhost:8080
    grafana:
        loadBalancer:
            servers:
                - url: http://localhost:3000

serversTransports:
    cockpit:
        insecureSkipVerify: true
EOT
$ sudo docker run -d --restart=always --net=host -v /var/lib/traefik/:/var/lib/traefik -v /etc/passwd:/etc/passwd:ro
$ sudo ufw allow 'DNS'
$ sudo ufw allow 'WWW'
$ sudo ufw allow 'WWW Secure' # Now visit https://cockpit.felixs-sdi1.alphahorizon.io/
$ sudo ufw allow '8443/tcp'
$ ssh pojntfx@felixs-sdi1.alphahorizon.io # Connect using SSH without Traefik
$ ssh -p 8443 pojntfx@felixs-sdi1.alphahorizon.io # Connect using SSH over Traefik without Traefik
$ ssh -o ProxyCommand="openssl s_client -connect ssh.felixs-sdi1.alphahorizon.io:443 -quiet" pojntfx@felixs-sdi1.alphahorizon.io

```

8 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

sudo sed -i /lib/systemd/system/cockpit.socket -e 's/ListenStream=9090/ListenStream=9091/g'

```

```
sudo systemctl daemon-reload
```

9 DNS

9.1 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 following at the end of the options block
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'
zone "example.pojtinger" {
    type master;
    file "/etc/bind/db.example.pojtinger";
    allow-query { any; };
    allow-transfer { 159.223.25.154; 2a03:b0c0:3:d0::1092:b001; };
};
```

```
zone "70.68.138.in-addr.arpa" {
    type master;
    file "/etc/bind/db.70.68.138";
    allow-query { any; };
    allow-transfer { 159.223.25.154; 2a03:b0c0:3:d0::1092:b001; };
};
```

```
zone "1.0.0.5.4.3.e.0.0.0.0.0.0.0.0.0.0.d.0.0.3.0.0.0.0.c.0.b.3.0.a.2.ip6.arpa" {
    type master;
    file "/etc/bind/db.1.0.0.5.4.3.e.0.0.0.0.0.0.0.0.0.0.d.0.0.3.0.0.0.0.c.0.b.3.0.a.2";
    allow-query { any; };
    allow-transfer { 159.223.25.154; 2a03:b0c0:3:d0::1092:b001; };
};
EOT
```

```
# Increase `1634570712` by one and reload after each change to propagate changes to the world
sudo tee /etc/bind/db.example.pojtinger <<'EOT'
```

```
$ORIGIN example.pojtinger.  
$TTL 3600
```

```
example.pojtinger.      IN      SOA      ns1.example.pojtinger. hostmaster.example.pojtinger.  
  
example.pojtinger.      IN      NS       ns1.example.pojtinger.  
example.pojtinger.      IN      NS       ns2.example.pojtinger.  
  
example.pojtinger.      IN      A        138.68.70.72  
example.pojtinger.      IN      AAAA     2a03:b0c0:3:d0::e34:5001  
  
ns1.example.pojtinger.  IN      A        138.68.70.72  
ns1.example.pojtinger.  IN      AAAA     2a03:b0c0:3:d0::e34:5001  
  
ns2.example.pojtinger.  IN      A        159.223.25.154  
ns2.example.pojtinger.  IN      AAAA     2a03:b0c0:3:d0::1092:b001  
  
example.pojtinger.      IN      MX       1          fb.mail.gandi.net.  
www.example.pojtinger.  IN      CNAME    example.pojtinger.  
EOT
```

```
# Increase `1634570724` by one and reload after each change to propagate changes to the world  
sudo tee /etc/bind/db.70.68.138 <<'EOT'  
$ORIGIN 70.68.138.in-addr.arpa.  
$TTL 3600
```

```
@      IN      SOA      ns1.example.pojtinger. hostmaster.example.pojtinger.      ( 1634570724  
  
@      IN      NS       ns1.example.pojtinger.  
@      IN      NS       ns2.example.pojtinger.  
  
72     IN      PTR      example.pojtinger.  
EOT
```

```
# Increase `1634570724` by one and reload after each change to propagate changes to the world  
sudo tee /etc/bind/db.1.0.0.5.4.3.e.0.0.0.0.0.0.0.0.0.0.0.0.d.0.0.3.0.0.0.0.c.0.b.3.0.a.2 <<'EOT'  
$ORIGIN 1.0.0.5.4.3.e.0.0.0.0.0.0.0.0.0.0.0.0.d.0.0.3.0.0.0.0.c.0.b.3.0.a.2.ip6.arpa.  
$TTL 3600
```

```
@      IN      SOA      ns1.example.pojtinger. hostmaster.example.pojtinger.      ( 1634570724  
  
@      IN      NS       ns1.example.pojtinger.  
@      IN      NS       ns2.example.pojtinger.  
  
1.0.0.5.4.3.e.0.0.0.0.0.0.0.0.0.0.0.0.d.0.0.3.0.0.0.0.c.0.b.3.0.a.2.ip6.arpa.      IN      PTR  
EOT
```

```
sudo named-checkconf
```

```
sudo named-checkzone example.pojtinger /etc/bind/db.example.pojtinger
```

```
sudo named-checkzone 70.68.138.in-addr.arpa. /etc/bind/db.70.68.138
```

```
sudo named-checkzone 1.0.0.5.4.3.e.0.0.0.0.0.0.0.0.0.d.0.0.3.0.0.0.0.c.0.b.3.0.a.2.ip6.arpa
```

```
sudo systemctl reload named
```

9.2 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 at the end of the options block
```

```
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'
```

```
zone "example.pojtinger" {
```

```
    type slave;
```

```
    file "db.example.pojtinger";
```

```
    allow-query { any; };
```

```
    masters { 138.68.70.72; 2a03:b0c0:3:d0::e34:5001; };
```

```
};
```

```
zone "70.68.138.in-addr.arpa" {
```

```
    type slave;
```

```
    file "db.70.68.138";
```

```
    allow-query { any; };
```

```
    masters { 138.68.70.72; 2a03:b0c0:3:d0::e34:5001; };
```

```
};
```

```
zone "1.0.0.5.4.3.e.0.0.0.0.0.0.0.0.0.d.0.0.3.0.0.0.0.c.0.b.3.0.a.2.ip6.arpa" {
```

```
    type slave;
```

```
    file "db.1.0.0.5.4.3.e.0.0.0.0.0.0.0.0.0.d.0.0.3.0.0.0.0.c.0.b.3.0.a.2";
```

```
    allow-query { any; };
```

```
    masters { 138.68.70.72; 2a03:b0c0:3:d0::e34:5001; };
```

```
};
```

EOT

```
sudo named-checkconf
sudo systemctl reload named
```

9.3 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       138.68.70.72
$ dig +noall +answer @138.68.70.72 example.pojtinger AAAA
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.pojtinger A
example.pojtinger.      3600    IN      A       138.68.70.72
$ dig +noall +answer @159.223.25.154 example.pojtinger AAAA
example.pojtinger.      3600    IN      AAAA    2a03:b0c0:3:d0::e34:5001
```

```
# Get NS record
$ dig +noall +answer @159.223.25.154 example.pojtinger NS
example.pojtinger.      3600    IN      NS      ns1.example.pojtinger.
example.pojtinger.      3600    IN      NS      ns2.example.pojtinger.
```

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

```
# Do IPv4 reverse lookup
$ dig +short @159.223.25.154 -x 138.68.70.72
example.pojtinger.
```

```
# Do IPv6 reverse lookup
$ dig +short @159.223.25.154 -x '2a03:b0c0:3:d0::e34:5001'
example.pojtinger.
```

Enable recursive queries to parent nameservers enabling your name-server to resolve external machines like `www.w3.org` by delegation.

```
# Get AAAA record for felix.pojtinger.com using parent nameservers
$ dig +noall +answer @159.223.25.154 felix.pojtinger.com AAAA
felix.pojtinger.com.    123     IN      CNAME   cname.vercel-dns.com.
```

Provide a mail exchange record pointing to `mx1.hdm-stuttgart.de`.

Test this configuration using dig accordingly.

```
# Get MX record
$ dig +noall +answer @159.223.25.154 example.pojtinger MX
example.pojtinger.      3600    IN      MX      1 fb.mail.gandi.net.
```

10 LDAP

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

```
sudo dpkg-reconfigure slapd # ldap.felixs-sdi1.alphahorizon.io, felixs-sdi1
```

```
curl ldaps://ldap.felixs-sdi1.alphahorizon.io:443 # Test the connection
```

```
socat tcp-listen:8389,fork openssl:ldap.felixs-sdi1.alphahorizon.io:443 # Run this on the laptop
curl ldap://localhost:8389 # Test the proxy's connection
```

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

```
# Connect with ldapwhoami like so:
ldapwhoami -H 'ldaps://ldap.felixs-sdi1.alphahorizon.io:443' -x # Anonymous
ldapwhoami -H 'ldaps://ldap.felixs-sdi1.alphahorizon.io:443' -W -D cn=admin,dc=ldap,dc=felixs-sdi1,dc=alphahorizon,dc=io
```

```
# Now add the objects (you can create a password hash using `slappasswd | base64`):
ldapadd -H 'ldaps://ldap.felixs-sdi1.alphahorizon.io:443' -W -D cn=admin,dc=ldap,dc=felixs-sdi1,dc=alphahorizon,dc=io
version: 1
```

```
dn: dc=ldap,dc=felixs-sdi1,dc=alphahorizon,dc=io
objectClass: dcObject
objectClass: organization
objectClass: top
dc: ldap
o: felixs-sdi1
```

```
# We already set this up using `dpkg-reconfigure`
# dn: cn=admin,dc=ldap,dc=felixs-sdi1,dc=alphahorizon,dc=io
# objectClass: organizationalRole
# objectClass: simpleSecurityObject
# cn: admin
# userPassword:: e1NTSEF9cEhFKOVQT0cyZ3lSeU9nanZGcXNXT2I1ekdzR2w5Q0Q=
```

```

# description: LDAP administrator

dn: ou=departments,dc=ldap,dc=felixs-sdi1,dc=alphahorizon,dc=io
objectClass: organizationalUnit
objectClass: top
ou: departments

dn: ou=software,ou=departments,dc=ldap,dc=felixs-sdi1,dc=alphahorizon,dc=io
objectClass: organizationalUnit
objectClass: top
ou: software

dn: ou=financial,ou=departments,dc=ldap,dc=felixs-sdi1,dc=alphahorizon,dc=io
objectClass: organizationalUnit
objectClass: top
ou: financial

dn: ou=devel,ou=software,ou=departments,dc=ldap,dc=felixs-sdi1,dc=alphahorizon,dc=io
objectClass: organizationalUnit
objectClass: top
ou: devel

dn: ou=testing,ou=software,ou=departments,dc=ldap,dc=felixs-sdi1,dc=alphahorizon,dc=io
objectClass: organizationalUnit
objectClass: top
ou: testing

dn: ou=ops,ou=software,ou=departments,dc=ldap,dc=felixs-sdi1,dc=alphahorizon,dc=io
objectClass: organizationalUnit
objectClass: top
ou: ops

dn: uid=bean,ou=devel,ou=software,ou=departments,dc=ldap,dc=felixs-sdi1,dc=alphahorizon,dc=io
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top
cn: Audrey Bean
sn: Bean
givenName: Audrey
mail: bean@ldap.felixs-sdi1.alphahorizon.io
uid: bean
userPassword:: e1NTSEF9NGxCMnc4dThQRXI5Rjd3VGZjN3ltNWkwUDk5N3d0eS8=

dn: uid=smith,ou=devel,ou=software,ou=departments,dc=ldap,dc=felixs-sdi1,dc=alphahorizon,dc=io
objectClass: inetOrgPerson

```

objectClass: organizationalPerson
objectClass: person
objectClass: top
cn: Jane Smith
sn: Smith
givenName: Jane
mail: smith@ldap.felixs-sdi1.alphahorizon.io
uid: smith
userPassword:: e1NTSEF9NGxCMnc4dThQRXI5Rjd3VGZjN3ltNWkwUDk5N3d0eS8=

dn: uid=waibel,ou=financial,ou=departments,dc=ldap,dc=felixs-sdi1,dc=alphahorizon,dc=io
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: posixAccount
objectClass: top
cn: Jakob Waibel
gidNumber: 100
homeDirectory: /usr/jakob
sn: Waibel
uid: waibel
uidNumber: 1337
givenName: Jakob
mail: waibel@ldap.felixs-sdi1.alphahorizon.io
userPassword:: e1NTSEF9NGxCMnc4dThQRXI5Rjd3VGZjN3ltNWkwUDk5N3d0eS8=

dn: uid=simpson,ou=financial,ou=departments,dc=ldap,dc=felixs-sdi1,dc=alphahorizon,dc=io
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top
cn: Homer Simpson
sn: Simpson
givenName: Homer
mail: simpson@ldap.felixs-sdi1.alphahorizon.io
uid: simpson
userPassword:: e1NTSEF9NGxCMnc4dThQRXI5Rjd3VGZjN3ltNWkwUDk5N3d0eS8=

dn: uid=pojtinger,ou=testing,ou=software,ou=departments,dc=ldap,dc=felixs-sdi1,dc=alphahorizon,dc=io
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top
cn: Felix Pojtinger
sn: Pojtinger
givenName: Felix

mail: pojtinger@ldap.felixs-sdi1.alphahorizon.io
uid: pojtinger
userPassword:: e1NTSEF9NGxCMnc4dThQRXI5Rjd3VGZjN3ltNWkwUDk5N3d0eS8=

dn: uid=simpson,ou=testing,ou=software,ou=departments,dc=ldap,dc=felixs-sdi1,dc=alphahorizon,
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top
cn: Maggie Simpson
sn: Simpson
givenName: Maggie
mail: simpson@ldap.felixs-sdi1.alphahorizon.io
uid: simpson
userPassword:: e1NTSEF9NGxCMnc4dThQRXI5Rjd3VGZjN3ltNWkwUDk5N3d0eS8=

dn: uid=aleimut,ou=devel,ou=software,ou=departments,dc=ldap,dc=felixs-sdi1,dc=alphahorizon,
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top
cn: Adelheit Aleimut
sn: Aleimut
givenName: Adelheit
mail: aleimut@ldap.felixs-sdi1.alphahorizon.io
uid: aleimut
userPassword:: e1NTSEF9NGxCMnc4dThQRXI5Rjd3VGZjN3ltNWkwUDk5N3d0eS8=

dn: uid=tibbie,ou=testing,ou=software,ou=departments,dc=ldap,dc=felixs-sdi1,dc=alphahorizon,
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: posixAccount
objectClass: top
cn: Oswald Tibbie
gidNumber: 100
homeDirectory: /usr/oswald
sn: Tibbie
uid: tibbie
uidNumber: 1234
givenName: Oswald
mail: tibbie@ldap.felixs-sdi1.alphahorizon.io
userPassword:: e1NTSEF9NGxCMnc4dThQRXI5Rjd3VGZjN3ltNWkwUDk5N3d0eS8=

dn: uid=operator,ou=ops,ou=software,ou=departments,dc=ldap,dc=felixs-sdi1,dc=alphahorizon,
objectClass: inetOrgPerson

```

objectClass: organizationalPerson
objectClass: person
objectClass: posixAccount
objectClass: top
cn: Operator Operatis
gidNumber: 100
homeDirectory: /usr/operator
sn: Operator
uid: operatis
uidNumber: 1235
givenName: Operator
mail: operator@ldap.felixs-sdi1.alphahorizon.io
userPassword:: e1NTSEF9Y1dtYUZ5Zi9HSTNTcFYyaktmYlpieUhEdFh5ek5wVEkK
EOT

```

```

# And test if we can access using a user
ldapwhoami -H 'ldaps://ldap.felixs-sdi1.alphahorizon.io:443' -W -D uid=bean,ou=devel,ou=soft

```

11 Apache

```

sudo apt update
sudo apt install -y apache2
sudo vi /etc/apache2/ports.conf # Now replace/add the following:
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.html /var/www/html # Replace the
sudo mkdir -p /var/www/sdidoc
sudo tree -T "Example Index For sdidoc" -H '.' -o /var/www/sdidoc/index.html /var/www/html #
sudo tee /etc/apache2/sites-available/apache.felixs-sdi1.alphahorizon.io.conf <<'EOT'
<VirtualHost *:8080>
    ServerName felixs-sdi1.alphahorizon.io
    ServerAlias apache.felixs-sdi1.alphahorizon.io

    ServerAdmin webmaster@alphahorizon.io
    DocumentRoot /var/www/html

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    <Directory "/var/www/html">
        Options Indexes FollowSymLinks
        AllowOverride None

```

```

        Require all granted
    </Directory>

    Alias /sdidoc /var/www/sdidoc

    <Directory "/var/www/sdidoc">
        Options Indexes FollowSymLinks
        AllowOverride None
        Require all granted
    </Directory>
</VirtualHost>
EOT
sudo a2dissite 000-default.conf
sudo a2ensite apache.felixs-sdi1.alphahorizon.io
sudo systemctl reload apache2

curl https://apache.felixs-sdi1.alphahorizon.io/ # Access the index
curl https://apache.felixs-sdi1.alphahorizon.io/sdidoc/ # Access the index in `/var/www/sdi

sudo apt install -y apache2-doc # Install the docs package
curl https://apache.felixs-sdi1.alphahorizon.io/manual/en/index.html # Access the installed

sudo mkdir -p /var/www/marx.apache.felixs-sdi1.alphahorizon.io
echo '<h1>Marx</h1>' | sudo tee /var/www/marx.apache.felixs-sdi1.alphahorizon.io/index.html
sudo tee /etc/apache2/sites-available/marx.apache.felixs-sdi1.alphahorizon.io.conf <<'EOT'
<VirtualHost *:8080>
    ServerName felixs-sdi1.alphahorizon.io
    ServerAlias marx.apache.felixs-sdi1.alphahorizon.io

    ServerAdmin webmaster@alphahorizon.io
    DocumentRoot /var/www/marx.apache.felixs-sdi1.alphahorizon.io

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    <Directory "/var/www/marx.apache.felixs-sdi1.alphahorizon.io">
        Options Indexes FollowSymLinks
        AllowOverride None
        Require all granted
    </Directory>
</VirtualHost>
EOT
sudo a2ensite marx.apache.felixs-sdi1.alphahorizon.io
sudo systemctl reload apache2

curl https://marx.apache.felixs-sdi1.alphahorizon.io/ # Access the Marx site

```

```

sudo mkdir -p /var/www/kropotkin.apache.felixs-sdi1.alphahorizon.io
echo '<h1>Kropotkin</h1>' | sudo tee /var/www/kropotkin.apache.felixs-sdi1.alphahorizon.io/
sudo tee /etc/apache2/sites-available/kropotkin.apache.felixs-sdi1.alphahorizon.io.conf <<'EOT
<VirtualHost *:8080>
    ServerName felixs-sdi1.alphahorizon.io
    ServerAlias kropotkin.apache.felixs-sdi1.alphahorizon.io

    ServerAdmin webmaster@alphahorizon.io
    DocumentRoot /var/www/kropotkin.apache.felixs-sdi1.alphahorizon.io

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    <Directory "/var/www/kropotkin.apache.felixs-sdi1.alphahorizon.io">
        Options Indexes FollowSymLinks
        AllowOverride None
        Require all granted
    </Directory>
</VirtualHost>
EOT
sudo a2ensite kropotkin.apache.felixs-sdi1.alphahorizon.io
sudo systemctl reload apache2

curl https://kropotkin.apache.felixs-sdi1.alphahorizon.io/ # Access the Kropotkin site

sudo mkdir -p /var/www/secure.apache.felixs-sdi1.alphahorizon.io
echo '<h1>Super secure content!</h1>' | sudo tee /var/www/secure.apache.felixs-sdi1.alphahorizon.io/
sudo tee /etc/apache2/sites-available/secure.apache.felixs-sdi1.alphahorizon.io.conf <<'EOT
<VirtualHost *:8080>
    ServerName felixs-sdi1.alphahorizon.io
    ServerAlias secure.apache.felixs-sdi1.alphahorizon.io

    ServerAdmin webmaster@alphahorizon.io
    DocumentRoot /var/www/secure.apache.felixs-sdi1.alphahorizon.io

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    <Directory "/var/www/secure.apache.felixs-sdi1.alphahorizon.io">
        Options Indexes FollowSymLinks
        AllowOverride None

        AuthType Basic
        AuthBasicProvider ldap
        AuthName "Please enter your LDAP username and password"
    </Directory>
</VirtualHost>
EOT

```

```

                                AuthLDAPURL "ldap://localhost:389/ou=devel,ou=software,ou=departments,dc=ld
                                Require valid-user
                                </Directory>
</VirtualHost>
EOT
sudo a2enmod authnz_ldap
sudo a2ensite secure.apache.felixs-sdi1.alphahorizon.io
sudo systemctl reload apache2

ldapwhoami -H 'ldap://localhost:389' -W -D uid=bean,ou=devel,ou=software,ou=departments,dc=ld

curl https://secure.apache.felixs-sdi1.alphahorizon.io/ # Try to access the secure site anon
curl -u bean:password https://secure.apache.felixs-sdi1.alphahorizon.io/ # Access the secure

```

12 MariaDB and phpMyAdmin

```

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

sudo mysql -u root -e 'GRANT ALL PRIVILEGES ON *.* TO 'phpmyadmin'@'localhost' WITH GRANT OPTION'

sudo apt install -y phpmyadmin libapache2-mod-php # apache2, y, yourpassword, yourpassword
sudo phpenmod mbstring

sudo a2disconf phpmyadmin

sudo tee /etc/apache2/sites-available/phpmyadmin.felixs-sdi1.alphahorizon.io.conf <<'EOT'
<VirtualHost *:8080>
    ServerName felixs-sdi1.alphahorizon.io
    ServerAlias phpmyadmin.felixs-sdi1.alphahorizon.io

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

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    <Directory "/usr/share/phpmyadmin">
        Options SymLinksIfOwnerMatch
        DirectoryIndex index.php

        # limit libapache2-mod-php to files and directories necessary by pma
        <IfModule mod_php7.c>
            php_admin_value upload_tmp_dir /var/lib/phpmyadmin/tmp

```

```

        php_admin_value open_basedir /usr/share/phpmyadmin/:/usr/share/doc/phpmyadm
    </IfModule>
</Directory>

# Disallow web access to directories that don't need it
<Directory "/usr/share/phpmyadmin/templates">
    Require all denied
</Directory>
<Directory "/usr/share/phpmyadmin/libraries">
    Require all denied
</Directory>
</VirtualHost>
EOT
sudo a2ensite phpmyadmin.felixs-sdi1.alphahorizon.io
sudo systemctl reload apache2

# Now visit https://phpmyadmin.felixs-sdi1.alphahorizon.io/ and login as root using yourpass

```

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

    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
        AllowOverride All
        Require all granted
        DirectoryIndex index.html
    </Directory>

    <Directory "/var/lib/ldap-account-manager/tmp">
        Options -Indexes
    </Directory>
</VirtualHost>

```

```

</Directory>

<Directory "/var/lib/ldap-account-manager/tmp/internal">
    Options -Indexes
    Require all denied
</Directory>

<Directory "/var/lib/ldap-account-manager/sess">
    Options -Indexes
    Require all denied
</Directory>

<Directory "/var/lib/ldap-account-manager/config">
    Options -Indexes
    Require all denied
</Directory>

<Directory "/usr/share/ldap-account-manager/lib">
    Options -Indexes
    Require all denied
</Directory>

<Directory "/usr/share/ldap-account-manager/help">
    Options -Indexes
    Require all denied
</Directory>

<Directory "/usr/share/ldap-account-manager/locale">
    Options -Indexes
    Require all denied
</Directory>
</VirtualHost>
EOT
sudo a2ensite ldap-account-manager.felixs-sdi1.alphahorizon.io
sudo systemctl reload apache2

# Now visit https://ldap-account-manager.felixs-sdi1.alphahorizon.io/templates/config/mainl
# - Don't encrypt session
# - Use `ldap://localhost:389/` as the server (where `ldaps://` is the default)
# - Set the new master password

# Now visit https://ldap-account-manager.felixs-sdi1.alphahorizon.io/templates/config/confma
# - Set `dc=ldap,dc=felixs-sdi1,dc=alphahorizon,dc=io` as the tree suffix
# - Set `cn=admin,dc=ldap,dc=felixs-sdi1,dc=alphahorizon,dc=io` as the list of valid users
# - Set SSH key file to empty string
# - Set the profile password to yourpassword

```

```
# - Set Users LDAP suffix under "Account types" to `ou=devel,ou=software,ou=departments,dc=1
# - Delete "groups" under "Account types"

# Now visit https://ldap-account-manager.felixs-sdi1.alphahorizon.io/templates/login.php and
```

14 Nextcloud

```
sudo apt update
sudo apt install -y libapache2-mod-php php-ctype php-curl php-dom php-gd php-iconv php-json

sudo mysql -u root -e "CREATE USER 'nextcloud'@'localhost' IDENTIFIED BY 'mypasswd';"
sudo mysql -u root -e "CREATE DATABASE nextcloud;"
sudo mysql -u root -e "GRANT ALL PRIVILEGES ON nextcloud.* TO 'nextcloud'@'localhost';"
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

curl -Lo /tmp/nextcloud.zip https://download.nextcloud.com/server/releases/nextcloud-23.0.0
unzip /tmp/nextcloud.zip 'nextcloud/*' -d /tmp/nextcloud
sudo mv /tmp/nextcloud/nextcloud/ /var/www/nextcloud.felixs-sdi1.alphahorizon.io/
sudo chown -R www-data:www-data /var/www/nextcloud.felixs-sdi1.alphahorizon.io/
sudo chmod -R 755 /var/www/nextcloud.felixs-sdi1.alphahorizon.io/

sudo tee /etc/apache2/sites-available/nextcloud.felixs-sdi1.alphahorizon.io.conf <<'EOT'
<VirtualHost *:8080>
    ServerName felixs-sdi1.alphahorizon.io
    ServerAlias nextcloud.felixs-sdi1.alphahorizon.io

    ServerAdmin webmaster@alphahorizon.io
    DocumentRoot /var/www/nextcloud.felixs-sdi1.alphahorizon.io

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    <Directory "/var/www/nextcloud.felixs-sdi1.alphahorizon.io">
        Options Indexes FollowSymLinks
        AllowOverride None
        Require all granted
    </Directory>
```



```

</VirtualHost>
EOT
sudo a2ensite nextcloud.felixs-sdi1.alphahorizon.io
sudo systemctl reload apache2

curl https://nextcloud.felixs-sdi1.alphahorizon.io/ # Access the Nextcloud installer

# Now visit https://nextcloud.felixs-sdi1.alphahorizon.io/index.php and create an admin account
# - Set `nextcloud` as the database user
# - Set `mypasswd` as the database password
# - Set `nextcloud` as the database name
# - Set `localhost:3306` as the database host
# - Click on "finish setup"
# - Visit https://nextcloud.felixs-sdi1.alphahorizon.io/index.php/settings/admin/richtextdocument
# - Visit https://nextcloud.felixs-sdi1.alphahorizon.io/index.php/settings/apps/installed/apps
# - Visit https://nextcloud.felixs-sdi1.alphahorizon.io/index.php/settings/admin/ldap and enable LDAP
# - Set `localhost` as the host
# - Set `389` as the port
# - Set `cn=admin,dc=ldap,dc=felixs-sdi1,dc=alphahorizon,dc=io` as the user DN
# - Set the password from `sudo dpkg-reconfigure slapd` as the password
# - Set `dc=ldap,dc=felixs-sdi1,dc=alphahorizon,dc=io` as the base DN
# Click verify, "continue", verify and "continue"
# - Set `organizationUnit` under `Only these object classes:` in the groups settings
# - Click `Verify settings and count the groups`
# - Visit https://nextcloud.felixs-sdi1.alphahorizon.io/index.php/login and login as bean user

```

15 Prometheus

```

sudo apt update
sudo apt install -y prometheus

sudo systemctl enable --now prometheus

```

16 Grafana

```

sudo apt update
sudo apt install -y apt-transport-https software-properties-common

curl -L https://packages.grafana.com/gpg.key | sudo apt-key add -
echo 'deb https://packages.grafana.com/oss/deb stable main' | sudo tee -a /etc/apt/sources.list.d/grafana.list

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:
[log]
filters = ldap:debug
# Replace the `[smtp]` block with the following:
[smtp]
enabled = true
host = mail.gandi.net:465
user = felixs-sdi1@alphahorizon.io
password = OHUYaDNtd2VhZmhld29ONGgK
from_address = felixs-sdi1@alphahorizon.io
from_name = Grafana
ehlo_identity = grafana.felixs-sdi1.alphahorizon.io

sudo tee /etc/grafana/ldap.toml <<'EOT'
[[servers]]
host = "127.0.0.1"
port = 389
use_ssl = false
start_tls = false
ssl_skip_verify = false

bind_dn = "cn=admin,dc=ldap,dc=felixs-sdi1,dc=alphahorizon,dc=io"
bind_password = 'yourldapadminpasswordfromdpkgconfigure'
search_filter = "(uid=%s)"
#search_base_dns = ["dc=ldap,dc=felixs-sdi1,dc=alphahorizon,dc=io"] # If we were to use groups
search_base_dns = ["ou=ops,ou=software,ou=departments,dc=ldap,dc=felixs-sdi1,dc=alphahorizon,dc=io"]

[servers.attributes]
name = "givenName"
surname = "sn"
username = "cn"
member_of = "memberOf"
email = "email"

# Would be useful if we were to use groups
#[[servers.group_mappings]]
#group_dn = "ou=ops,ou=software,ou=departments,dc=ldap,dc=felixs-sdi1,dc=alphahorizon,dc=io"
#org_role = "Admin"

```

```

#
#[[servers.group_mappings]]
#group_dn = "ou=ops,ou=software,ou=departments,dc=ldap,dc=felixs-sdi1,dc=alphahorizon,dc=io"
#org_role = "Editor"
#
#[[servers.group_mappings]]
#group_dn = "*"
#org_role = "Viewer"

[[servers.group_mappings]]
group_dn = "*"
org_role = "Admin"
EOT

# Visit https://grafana.felixs-sdi1.alphahorizon.io/?orgId=1 and login as `operator` using t

# Now add a datasource, select Prometheus and use `http://localhost:9090` as the URL

# Now go to create, import and select `1860` as the ID (https://grafana.com/grafana/dashboards)

# Now go to Alerting, create alert with name `HostDiskWillFillIn24Hours` and type `Grafana m

# Now go to https://grafana.felixs-sdi1.alphahorizon.io/alerting/notifications/receivers/graf

```