Ansible Meetup at AWS Munich

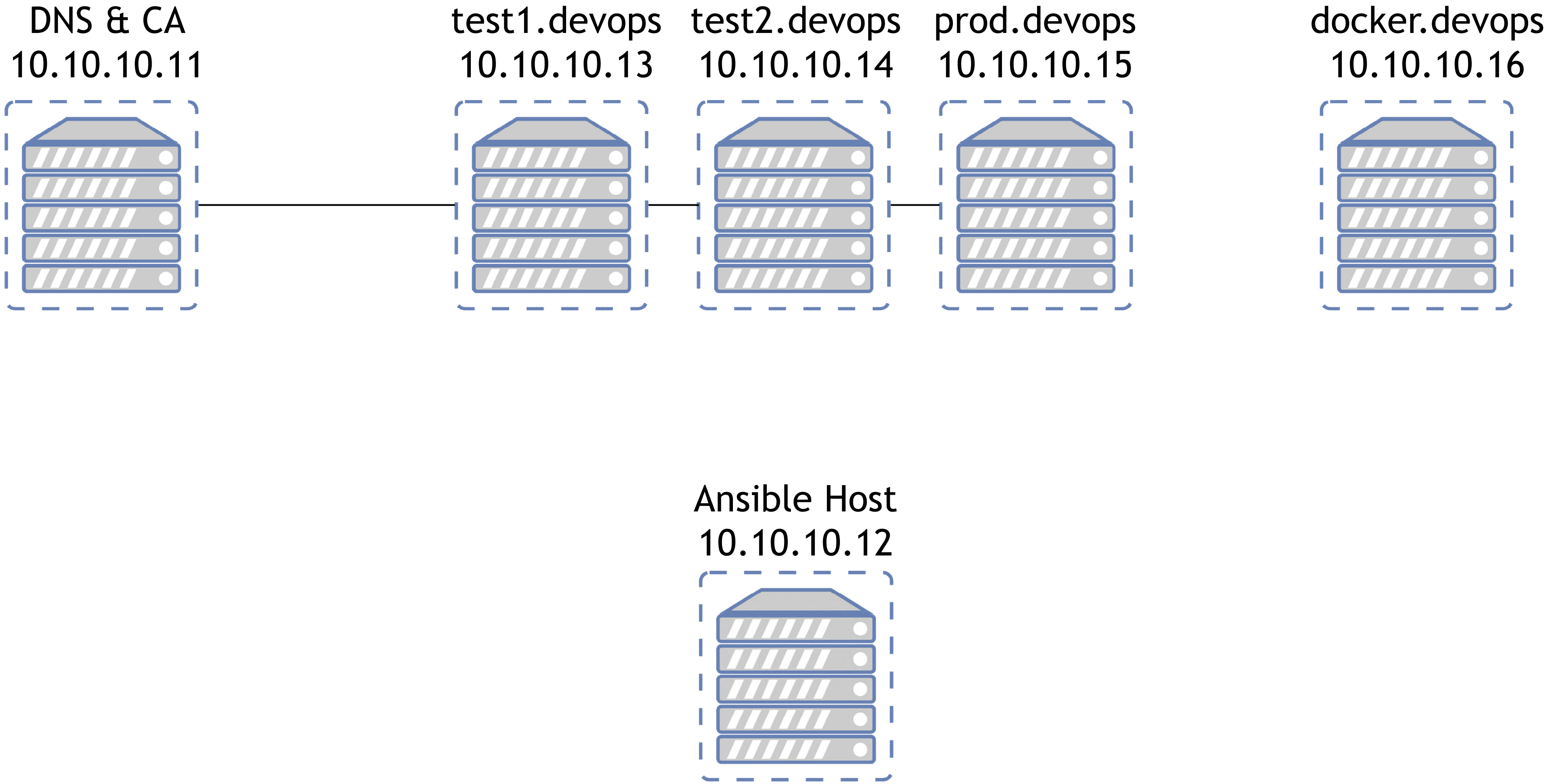
Managing Podman pods with Ansible

Stavros Tsirakidis

IT-OLOGIA

Informatik · Software · Consulting

- Podman in RHEL9
- From Docker Compose
  - To Managing Pods with Ansible



DNS & CA
10.10.10.11

test1.devops
10.10.10.13

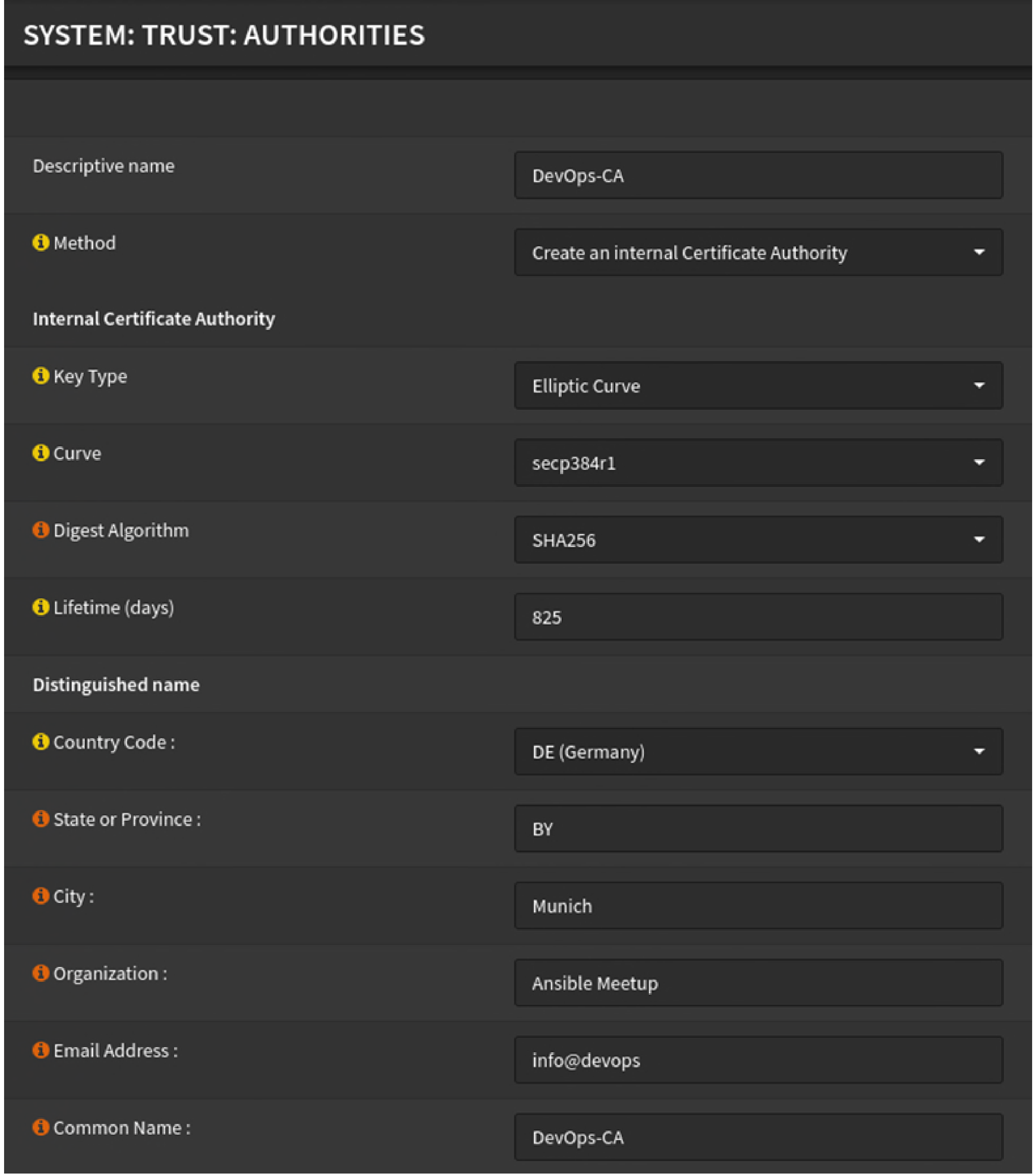
test2.devops
10.10.10.14

prod.devops
10.10.10.15

docker.devops
10.10.10.16

Ansible Host
10.10.10.12

Certificate Authority



SYSTEM: TRUST: AUTHORITIES

Descriptive name	DevOps-CA
Method	Create an internal Certificate Authority

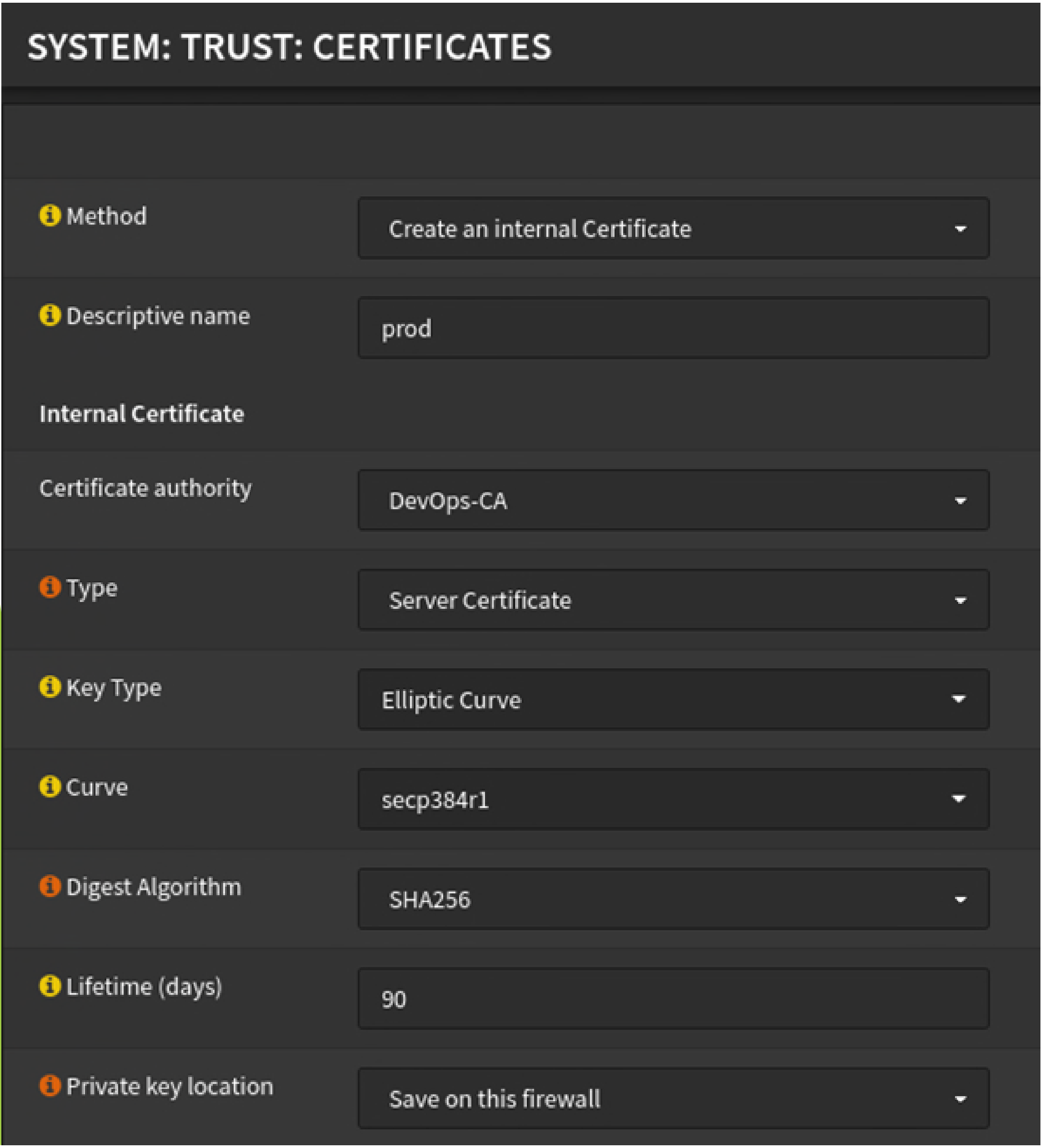
Internal Certificate Authority

Key Type	Elliptic Curve
Curve	secp384r1
Digest Algorithm	SHA256
Lifetime (days)	825

Distinguished name

Country Code :	DE (Germany)
State or Province :	BY
City :	Munich
Organization :	Ansible Meetup
Email Address :	info@devops
Common Name :	DevOps-CA

Internal Server Certificates

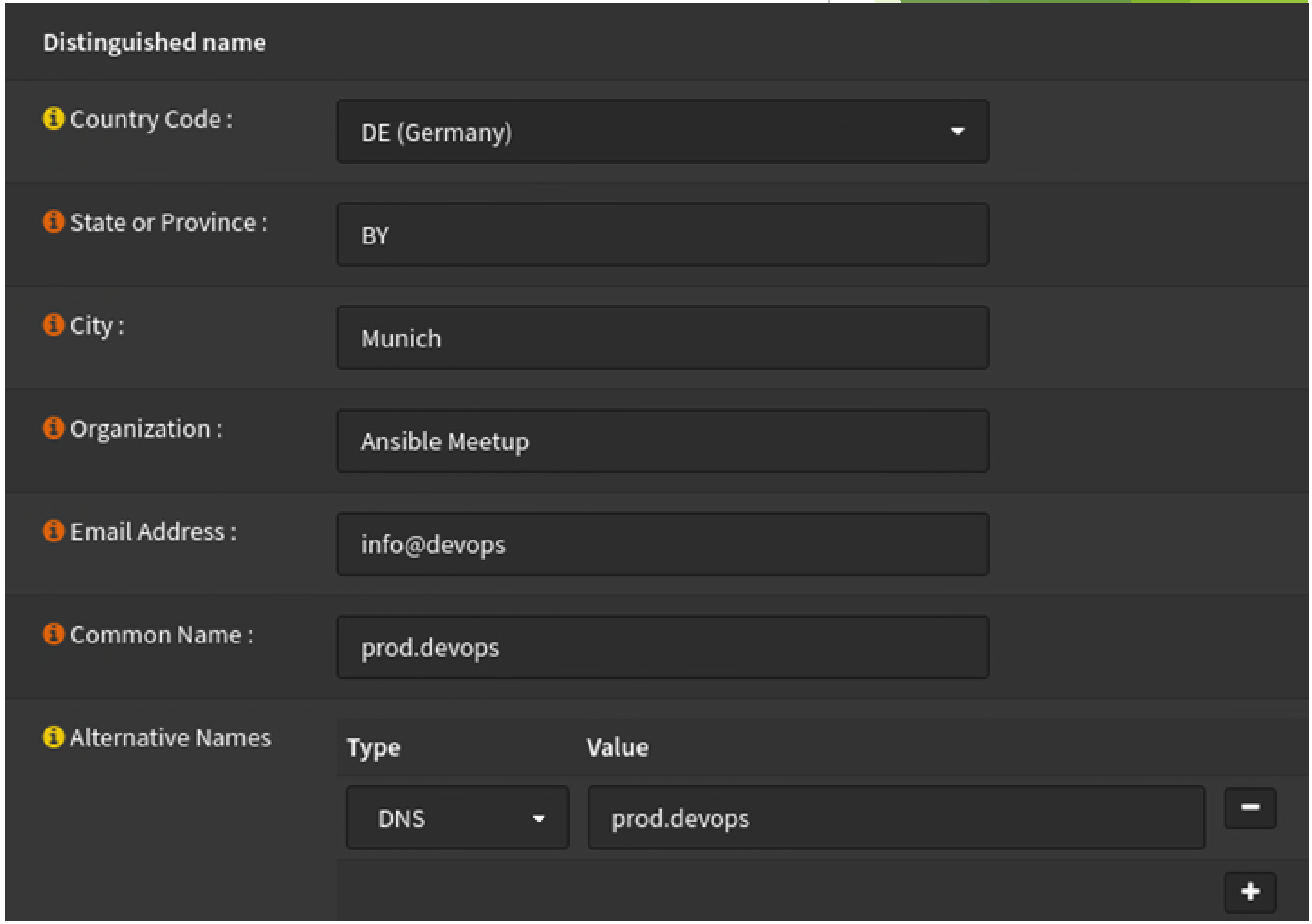


SYSTEM: TRUST: CERTIFICATES

Method	Create an internal Certificate
Descriptive name	prod

Internal Certificate

Certificate authority	DevOps-CA
Type	Server Certificate
Key Type	Elliptic Curve
Curve	secp384r1
Digest Algorithm	SHA256
Lifetime (days)	90
Private key location	Save on this firewall

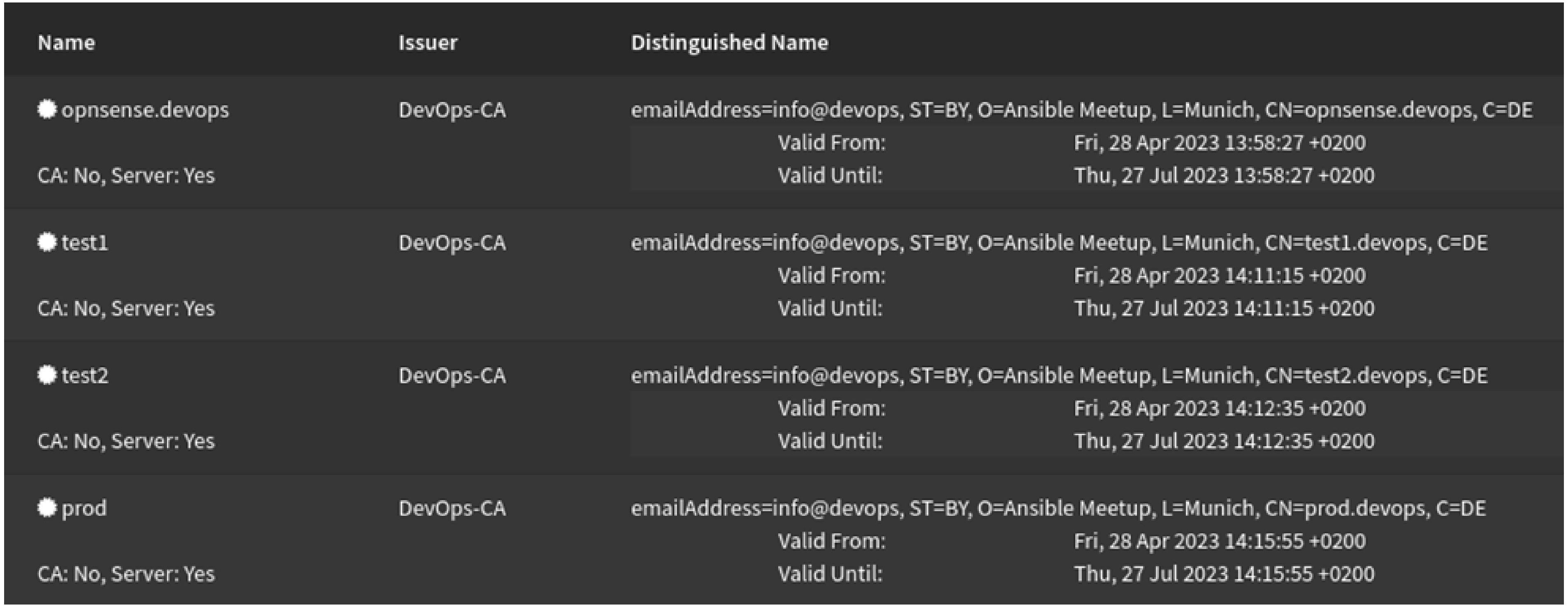


Distinguished name

Country Code :	DE (Germany)
State or Province :	BY
City :	Munich
Organization :	Ansible Meetup
Email Address :	info@devops
Common Name :	prod.devops

Alternative Names

Type	Value
DNS	prod.devops



Name	Issuer	Distinguished Name
opnsense.devops CA: No, Server: Yes	DevOps-CA	emailAddress=info@devops, ST=BY, O=Ansible Meetup, L=Munich, CN=opnsense.devops, C=DE Valid From: Fri, 28 Apr 2023 13:58:27 +0200 Valid Until: Thu, 27 Jul 2023 13:58:27 +0200
test1 CA: No, Server: Yes	DevOps-CA	emailAddress=info@devops, ST=BY, O=Ansible Meetup, L=Munich, CN=test1.devops, C=DE Valid From: Fri, 28 Apr 2023 14:11:15 +0200 Valid Until: Thu, 27 Jul 2023 14:11:15 +0200
test2 CA: No, Server: Yes	DevOps-CA	emailAddress=info@devops, ST=BY, O=Ansible Meetup, L=Munich, CN=test2.devops, C=DE Valid From: Fri, 28 Apr 2023 14:12:35 +0200 Valid Until: Thu, 27 Jul 2023 14:12:35 +0200
prod CA: No, Server: Yes	DevOps-CA	emailAddress=info@devops, ST=BY, O=Ansible Meetup, L=Munich, CN=prod.devops, C=DE Valid From: Fri, 28 Apr 2023 14:15:55 +0200 Valid Until: Thu, 27 Jul 2023 14:15:55 +0200

Docker Compose

```
---
version: "2"
services:
  bookstack:
    image: lscr.io/linuxserver/bookstack
    container_name: bookstack
    environment:
      - PUID=1000
      - PGID=1000
      - APP_URL=http://docker.devops:6875
      - DB_HOST=bookstack_db
      - DB_PORT=3306
      - DB_USER=bookstack
      - DB_PASS=bookstack
      - DB_DATABASE=bookstackapp
    volumes:
      - /home/devops/bookstack/bookstack_config:/config
    ports:
      - 6875:80
    restart: unless-stopped
    depends_on:
      - bookstack_db
  bookstack_db:
    image: lscr.io/linuxserver/mariadb
    container_name: bookstack_db
    environment:
      - PUID=1000
      - PGID=1000
      - MYSQL_ROOT_PASSWORD=bookstack
      - TZ=Europe/London
      - MYSQL_DATABASE=bookstackapp
      - MYSQL_USER=bookstack
      - MYSQL_PASSWORD=bookstack
    volumes:
      - /home/devops/bookstack/mariadb_config:/config
    restart: unless-stopped
```

Podman

- podman.io
- RHEL 9 documentation

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9

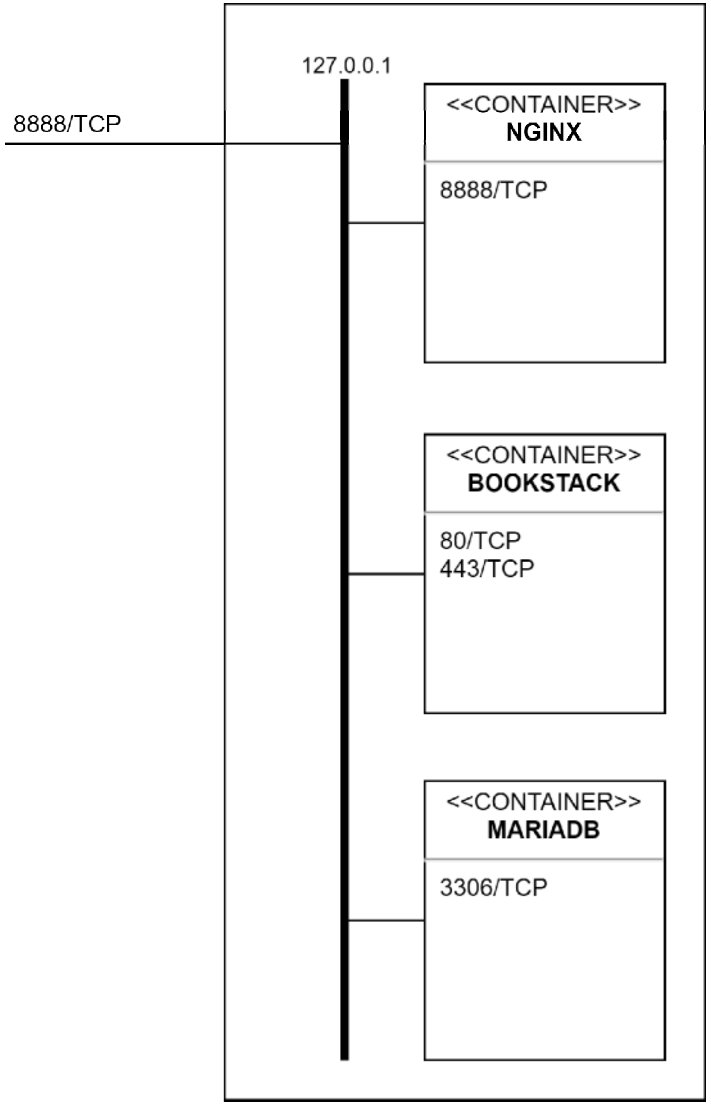
Building, running, and managing containers

Container Registries

- https://catalog.redhat.com/software/containers
  - Certified Images
  - UID provided in technical description

- https://hub.docker.com

BookStack POD



- All containers in a Podman pod share the same network namespace.
  - They will have the same IP address, MAC addresses, and port mappings.

- Containers communicate within the pod by using localhost (127.0.0.1).

- The port to be exposed is defined on the pod and not on the container.

Rootless Containers With Podman In Red Hat Enterprise Linux 9

- Containers run in user namespace

- SELinux in enforcing mode
  - podman unshare

- Privileged ports (1-1024) per default cannot be used
  - Exposed ports are not automatically opened in the firewall

Rootless Containers With Podman In Red Hat Enterprise Linux 9

- Containers run in user namespace

```
[devops@prod bookstack]$ sudo cat /etc/subuid
user:100000:65536
devops:165536:65536

[devops@prod bookstack]$ podman unshare cat /proc/self/uid_map
         0       1001          1
         1     165536      65536
[devops@prod bookstack]$ podman exec -it bookstack_http cat /proc/self/uid_map
         0       1001          1
         1     165536      65536
[devops@prod bookstack]$ podman exec -it bookstack_app cat /proc/self/uid_map
         0       1001          1
         1     165536      65536
[devops@prod bookstack]$ podman exec -it bookstack_db cat /proc/self/uid_map
         0       1001          1
         1     165536      65536
```

Rootless Containers With Podman In Red Hat Enterprise Linux 9

- Containers run in user namespace

```
[devops@prod bookstack]$ sudo cat /etc/subuid
user:100000:65536
devops:165536:65536

[devops@prod bookstack]$ ls -al
total 4
drwxrwxr-x. 6 devops devops  101 May  1 18:54 .
drwx------. 7 devops devops  187 May  1 19:36 ..
drwxrwxr-x. 7 166535 166535  112 May  1 18:53 bookstack_config
drwxrwxr-x. 4 166535 166535   52 May  1 18:53 mariadb_config
drwxr-xr-x. 3 165636 165636 4096 May  1 18:54 nginx_etcnginx
drwxr-xr-x. 3 165636 165636   65 May  1 18:54 nginx_etcsslprivate

MARIADB UID 1000     -> 165536 + 999 -> 166535
BOOKSTACK UID 1000   -> 165536 + 999 -> 166535
NGINX UID 101        -> 165536 + 100 -> 165636
```

Rootless Containers With Podman
In Red Hat Enterprise Linux 9

- SELinux in enforcing mode

podman unshare chown [OPTION] [PUID]:[PGID] FILE...

```
[devops@prod bookstack]$ ls -al
total 4
drwxrwxr-x. 6 devops devops  101 May  1 18:54 .
drwx------. 7 devops devops  187 May  1 19:36 ..
drwxrwxr-x. 7 166535 166535  112 May  1 18:53 bookstack_config
drwxrwxr-x. 4 166535 166535   52 May  1 18:53 mariadb_config
drwxr-xr-x. 3 165636 165636 4096 May  1 18:54 nginx_etcnginx
drwxr-xr-x. 3 165636 165636   65 May  1 18:54 nginx_etcsslprivate

[devops@prod bookstack]$ ls -ldZ bookstack_config/
drwxrwxr-x. 7 166535 166535 system_u:object_r:container_file_t:s0:c83,c348 112 May  1 18:53
```

Rootless Containers With Podman
In Red Hat Enterprise Linux 9

- Privileged ports (1-1024) per default cannot be used
    - Exposed ports are not automatically opened in the firewall

```
sudo firewall-cmd --permanent –add-port=8888/tcp
```