Splunk on K8s (EKS)

über mich

- Freelancer @ Batchworks

- Consulting, Trainings
- Splunk Architect, Administrator, Developer …
- Kubernetes Certified Application Developer (CKAD)
- CCI-V, CCE-V, CCP-V, CCA-V, CCIA, CCEE, VCP4, ITIL
- SME for XenDesktop7 and XenServer

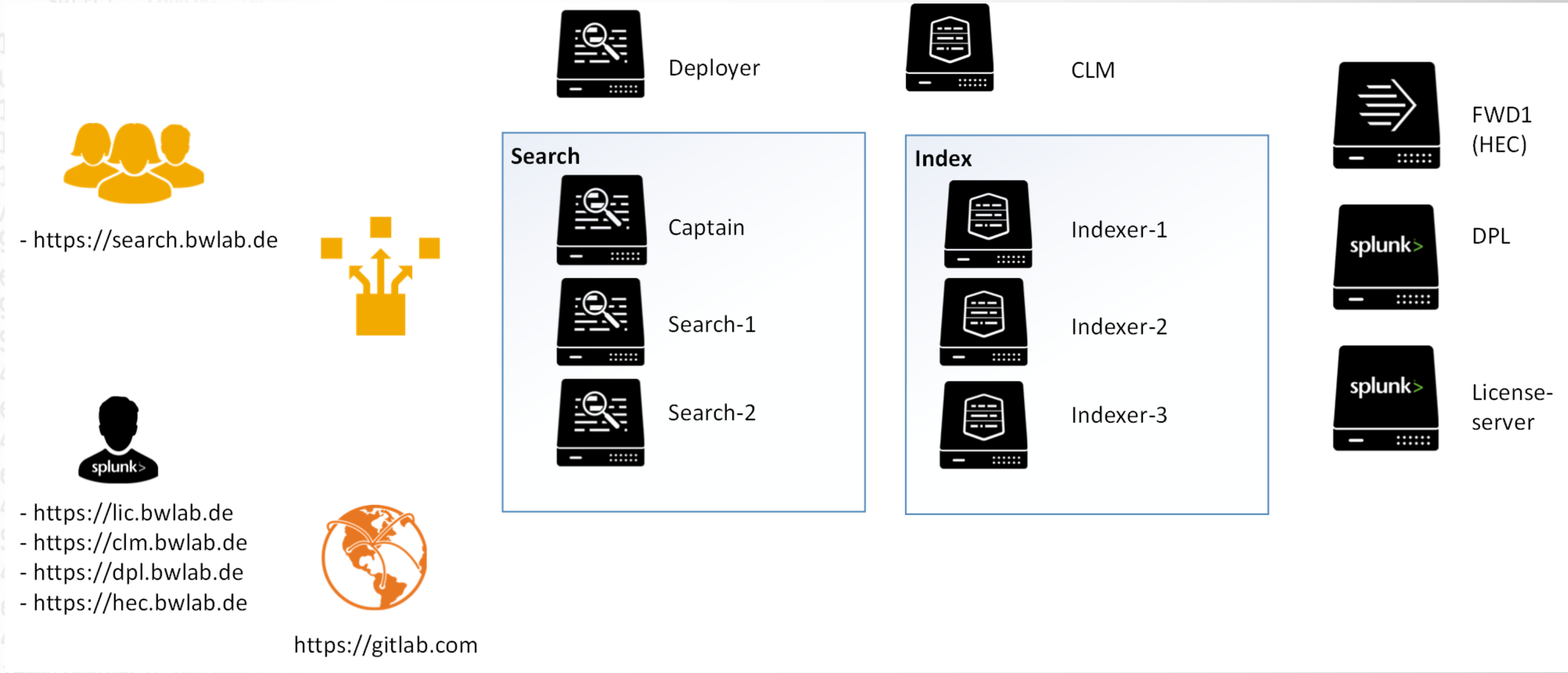
@schose

andreas@batchworks.de

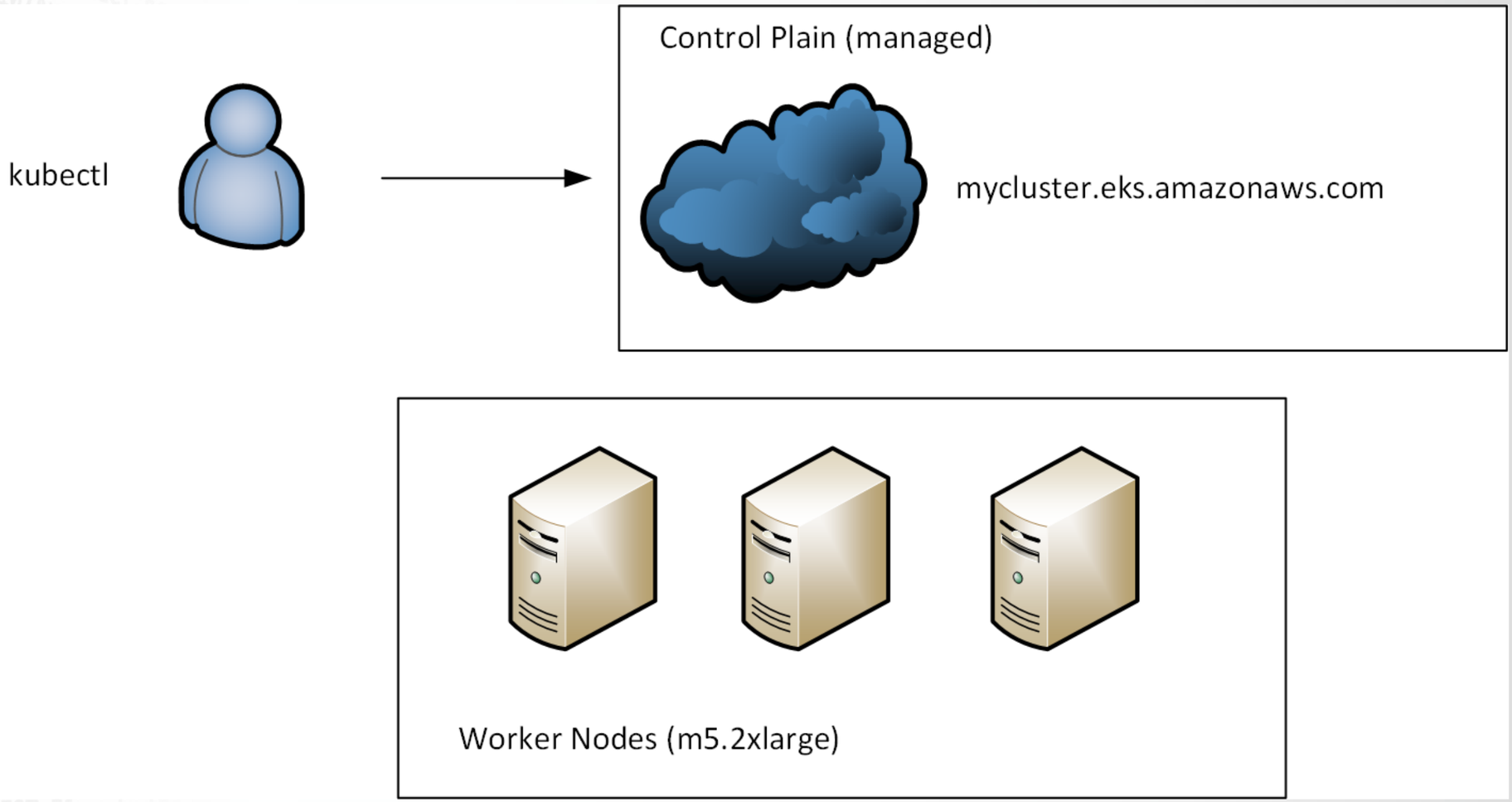
Agenda

- warum Splunk auf Kubernetes?
- Von Docker über Docker-compose zu Kubernetes
- Splunk auf EKS (Demo)
- Maintainance (Demo)
- Splunk Connect for Kubernetes

Warum Kubernetes? - Zielbild



Kubernets Überblick



Splunk Docker Image

- https://github.com/splunk/docker-splunk/

- „Support“:
https://www.splunk.com/blog/2018/10/24/announcing-splunk-on-docker.html

- docker run -d -p 8000:8000 -e SPLUNK_START_ARGS=--accept-license -e SPLUNK_PASSWORD=<password> splunk/splunk:latest
- ENV documentation:
https://splunk.github.io/splunk-ansible/ADVANCED.html#inventory-script

Docker Compose -> kubectl

docker-compose.yml

```
version: '3'
services:
clm:
  image: splunk/splunk:7.2.7
  ports:
   - "8001:8000"
   - "8002:8089"
   - "12011:22"
  volumes:
   - /docker/dockercompose/clm/etc:/opt/splunk/etc
   - /docker/dockercompose/clm/var:/opt/splunk/var
  hostname: clm
  environment:
   - SPLUNK_START_ARGS=--accept-license
   - SPLUNK_LICENSE_URI=http://localhost/splunk.lic
   - SPLUNK_PASSWORD=Splunkr0cks
   - SPLUNK_ROLE=splunk_cluster_master
   - SPLUNK_INDEXER_URL=idx1,idx2,idx3
   - SPLUNK_IDXC_SECRET=mypass4splunk

idx1:
  image: splunk/splunk:7.2.7
  ports:
   - "8011:8000"
   - "12021:22"
  volumes:
   - /docker/dockercompose/idx1/etc:/opt/splunk/etc
   - /docker/dockercompose/idx1/var:/opt/splunk/var
   - /docker/dockercompose/idx1/colddb:/colddb
```

pod.yml

```
spec:
  replicas: 1
  template:
    metadata:
      labels:
        app: splunk
        role: splunk_cluster_master
        tier: management
    spec:
      hostname: master
      containers:
        - name: master
          image: splunk/splunk:7.2.7
      envFrom:
          - configMapRef:
              name: splunk-config
        env:
          - name: SPLUNK_ROLE
            value: splunk_cluster_master
        ports:
          - name: web
            containerPort: 8000
          - name: mgmt
            containerPort: 8089
        volumeMounts:
          - name: splunk-master-data
            mountPath: /opt/splunk/var
          - name: splunk-master-config
            mountPath: /opt/splunk/etc
          - name: splunk-defaults-configmap
            mountPath: /tmp/defaults
      volumes:
        - name: splunk-master-config
          persistentVolumeClaim:
            claimName: splunk-master-config
...
```

Storage

docker-compose.yml

```
volumes:
  - /docker/dockercompose/clm/etc:/opt/splunk/etc
  - /docker/dockercompose/clm/var:/opt/splunk/var
```

pod.yml

```
    containers:
      - name: master
        image: splunk/splunk:7.2.7
        volumeMounts:
          - name: splunk-master-data
            mountPath: /opt/splunk/var
          - name: splunk-master-config
            mountPath: /opt/splunk/etc
    volumes:
      - name: splunk-master-config
        persistentVolumeClaim:
          claimName: splunk-master-config
      - name: splunk-master-data
        persistentVolumeClaim:
          claimName: splunk-master-data
```

pvc.yml

```
---
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: splunk-master-data
  labels:
    app: splunk
    role: splunk_cluster_master
    tier: management
spec:
  accessModes:
  - ReadWriteOnce
  resources:
    requests:
      storage: 20Gi
```

Demo

Demo

- Configmap erstellen (ENV + defaults.yml)
- docker run --rm -it splunk/splunk:latest create-defaults > default.yml
- PVC erstellen
- Service erstellen
- Pod erstellen
- Config per WebGUI Prüfen

Run(!!!)

Apps deployen

- Indexer hinzufügen
- Apps auf SHC, DPL, CLM
- Upgrade Splunk

Splunk upgraden

pod.yml

```
containers:
    - name: master
      image: splunk/splunk:7.2.7
      envFrom:
        - configMapRef:
            name: splunk-config
      env:
        - name: SPLUNK_ROLE
          value: splunk_cluster_master
```

Splunk Connect for Kubernetes

pod.yml

```
containers:
    - name: master
      image: splunk/splunk:7.2.7
      envFrom:
        - configMapRef:
            name: splunk-config
      env:
        - name: SPLUNK_ROLE
          value: splunk_cluster_master
```

Splunk Connect for Kubernetes

- Helm charts
- https://github.com/splunk/splunk-connect-for-kubernetes
- Logging
- Objects
- Metrics
- helm install --name my-splunk-objects -f objects.yaml https://github.com/splunk/splunk-connect-for-kubernetes/releases/download/1.2.0/splunk-kubernetes-objects-1.2.0.tgz

Fragen??