Project: Guestbook (Docker → Kubernetes) — Full Professional Documentation

---

Table of contents

---

1 — Executive summary

The Guestbook project is a simple web front-end (HTTP on port **3000**) that accepts text entries and displays them. For the lab you:

- Build a container image (multi-stage Docker) → push to IBM Cloud Container Registry (icr).
- Deploy with a Kubernetes **Deployment** (single container).
- Enable **Horizontal Pod Autoscaler (HPA)** to scale pods based on CPU.
- Perform **rolling updates** to the app (v1 → v2) and demonstrate **rollback** to a prior revision.

This document makes the deployment reproducible, secure, and monitorable from a SOC perspective — with detection rules, MITRE mapping, and a Tier-3 incident runbook.

2 — Goals & success criteria

Technical goals

- Build and push a functioning guestbook image: `us.icr.io/<namespace>/guestbook:v1`.
- Deploy `guestbook` Deployment ⇒ verify app reachable via `kubectl port-forward` on `localhost:3000`.
- Create an HPA that scales between `min=1` and `max=10` pods based on CPU (50% target).
- Update app to v2, perform rolling update, confirm rollout history, then rollback to revision 1.

Security & SOC goals

- Image scanned before deploy; CI enforces fail-on-high-severity vulnerabilities.
- Pod security posture set (non-root, readOnlyRootFilesystem, no privileged).
- Telemetry flows into a SIEM/observability stack (container logs, K8s audit, node/syslogs, metrics) for detection and incident investigation.
- Provide detection content (Splunk & Falco) and a Tier-3 runbook for live incidents.

---

3 — Environment & prerequisites (tools + why they matter)

Minimum tools (versions matter; use up-to-date releases)

- `kubectl` — Kubernetes CLI (match cluster version). Used for deploy, port-forward, troubleshooting. Kubernetes
- `docker` or Buildx — for local image build / multi-stage builds.
- `ibmcloud` CLI + Container Registry plugin (lab uses `ibmcloud cr images`). (lab instructions reference `ibmcloud cr images`)
- Kubernetes cluster with ability to create Deployments, Services, HPA, and access metrics (see metrics server note below).
- `metrics-server` (or provider of metrics) installed in the cluster — **HPA requires metrics** to make scaling decisions. Without metrics-server (or an alternative metrics provider), HPA cannot read CPU usage. MediumKubernetes

Recommended observability + runtime security

- Centralized logs: e.g., Splunk (Splunk Connect for Kubernetes), ELK, or cloud logging (GCP/Azure/IBM). Splunk provides prebuilt Kubernetes detection content. research.splunk.com

- Runtime security: Falco (eBPF) to detect reverse shells, unexpected execs, privileged containers, etc. Falco maps well into SIEM for near-real-time alerts. Sysdigfalcosecurity.github.io

---

4 — Source artifacts & build steps

Repo layout (typical)

```
pgsql

guestbook/
  v1/
    guestbook/
      Dockerfile
      index.html
      package.json
      server.js  # example node app binding to 3000
  k8s/
    deployment.yml
    service.yml
    hpa.yml
  README.md
```

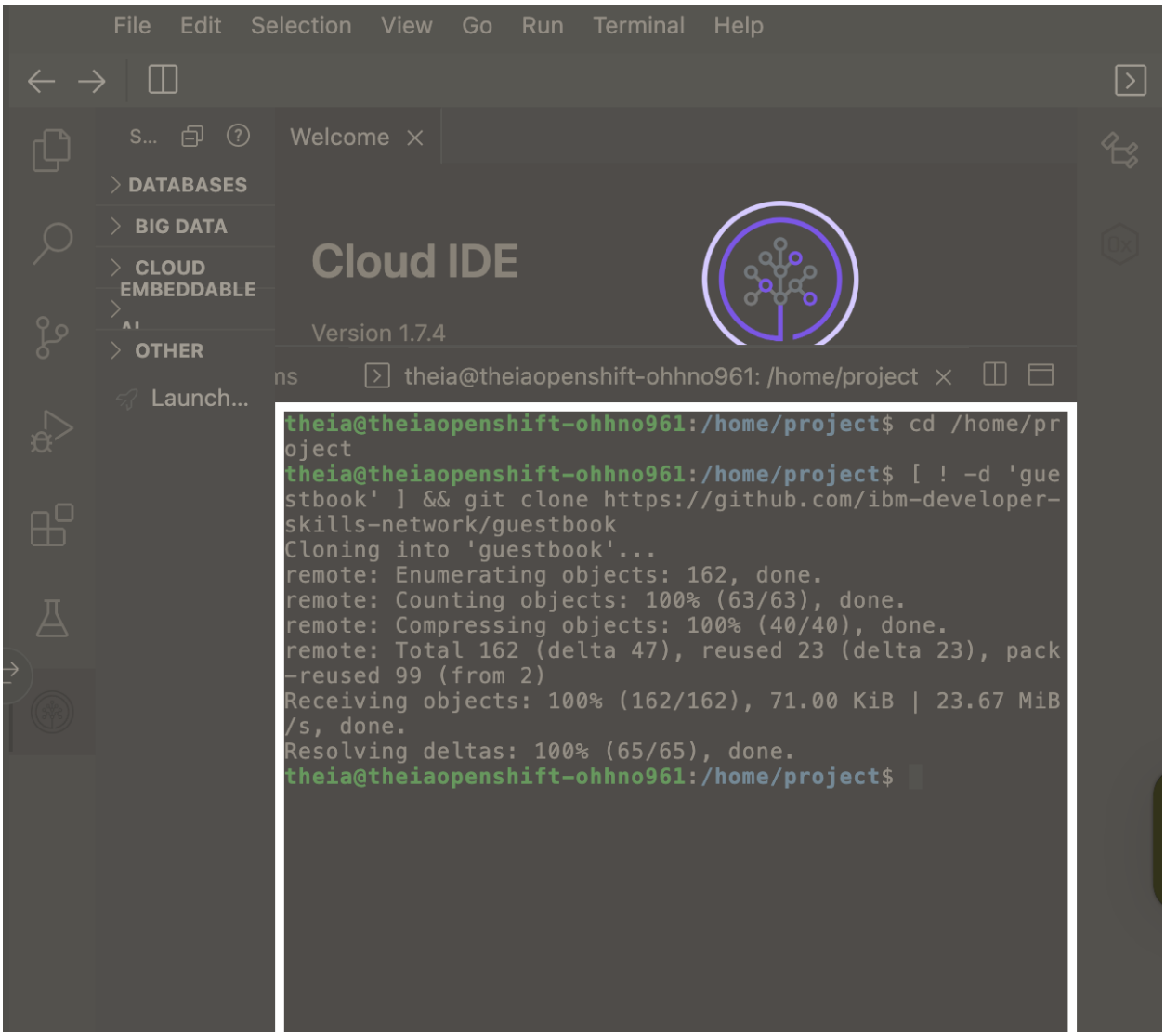
Dockerfile — multi-stage example (Node.js guestbook)

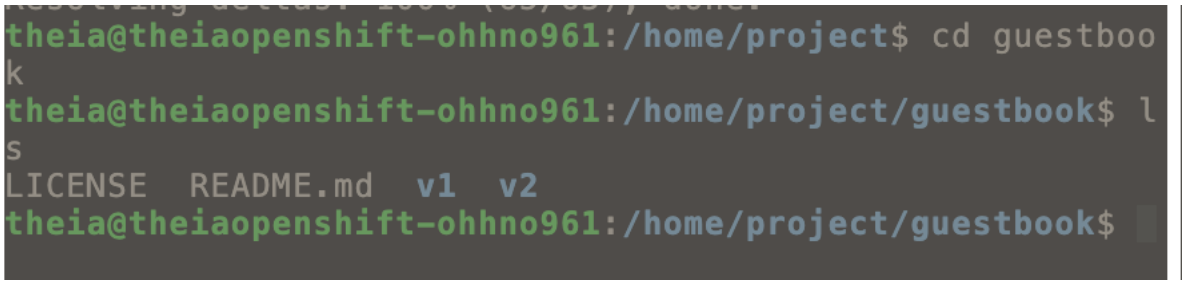
Use multi-stage to reduce image size and separate build/runtime. Also build as non-root and avoid unnecessary packages.

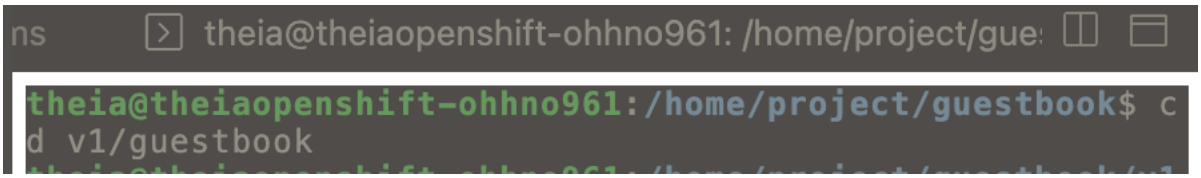
```
dockerfile
# stage: builder
FROM node:18-alpine AS builder
WORKDIR /app
COPY package*.json ./
RUN npm ci --production=false
COPY . .
RUN npm run build || true

# stage: runtime (minimal)
FROM node:18-alpine AS runtime
# create non-root user
RUN addgroup -S app && adduser -S app -G app
WORKDIR /app
COPY --from=builder /app ./
# set ownership to non-root
RUN chown -R app:app /app
USER app
ENV NODE_ENV=production
EXPOSE 3000
CMD ["node", "server.js"]
```

Notes:

- `npm ci` is used for reproducible installs (locks are respected).
- Run as a non-root user — important for Pod security. (see hardening).
- Multi-stage avoids shipping build tools to runtime image.







5 — Build & push image (IBM Cloud Container Registry example)

Set namespace environment variable (lab):

```
bash
export MY_NAMESPACE=sn-labs-$USERNAME
```

Build & tag:

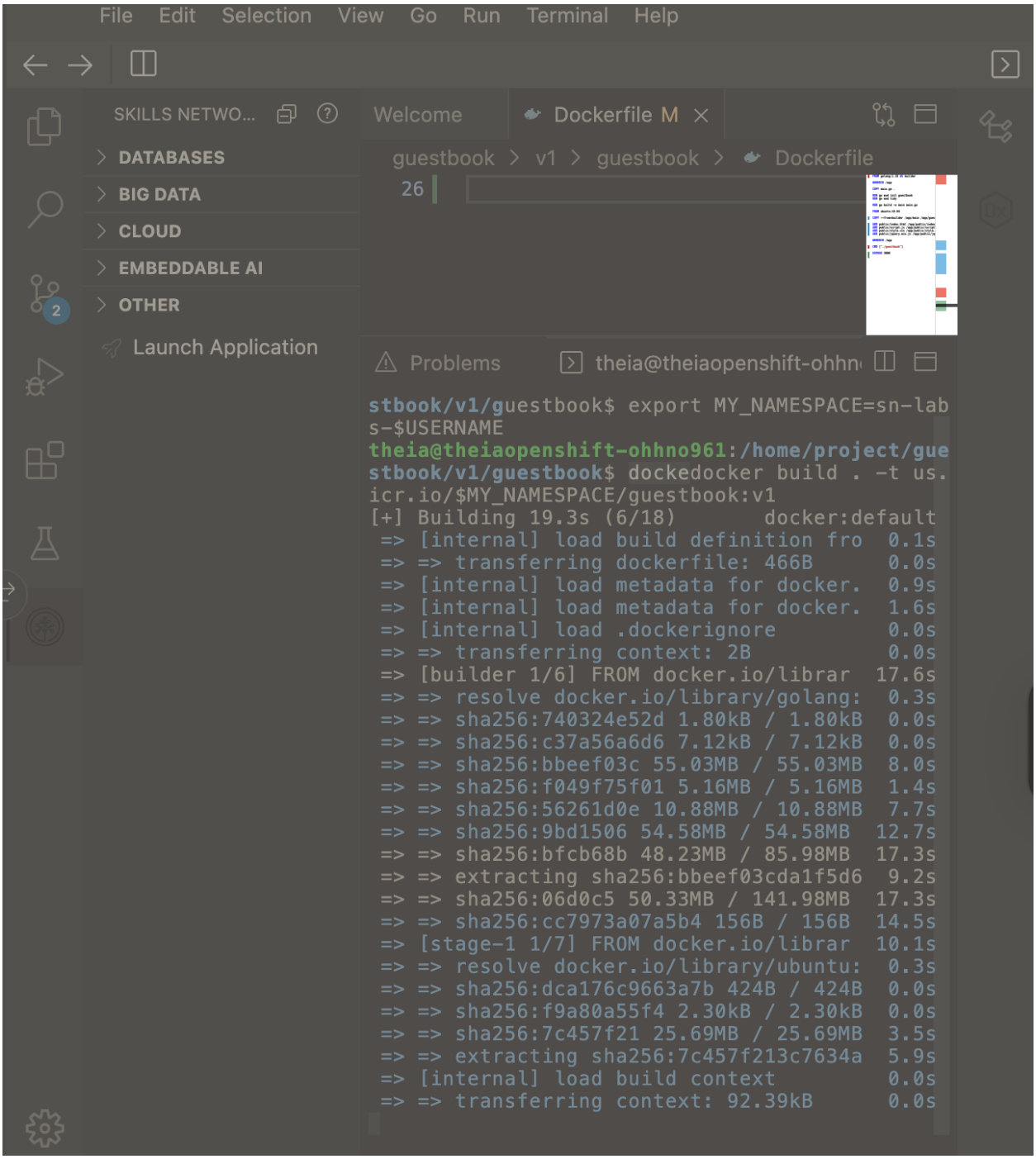
```
bash
docker build -t us.icr.io/${MY_NAMESPACE}/guestbook:v1 ./v1/guestbook
```

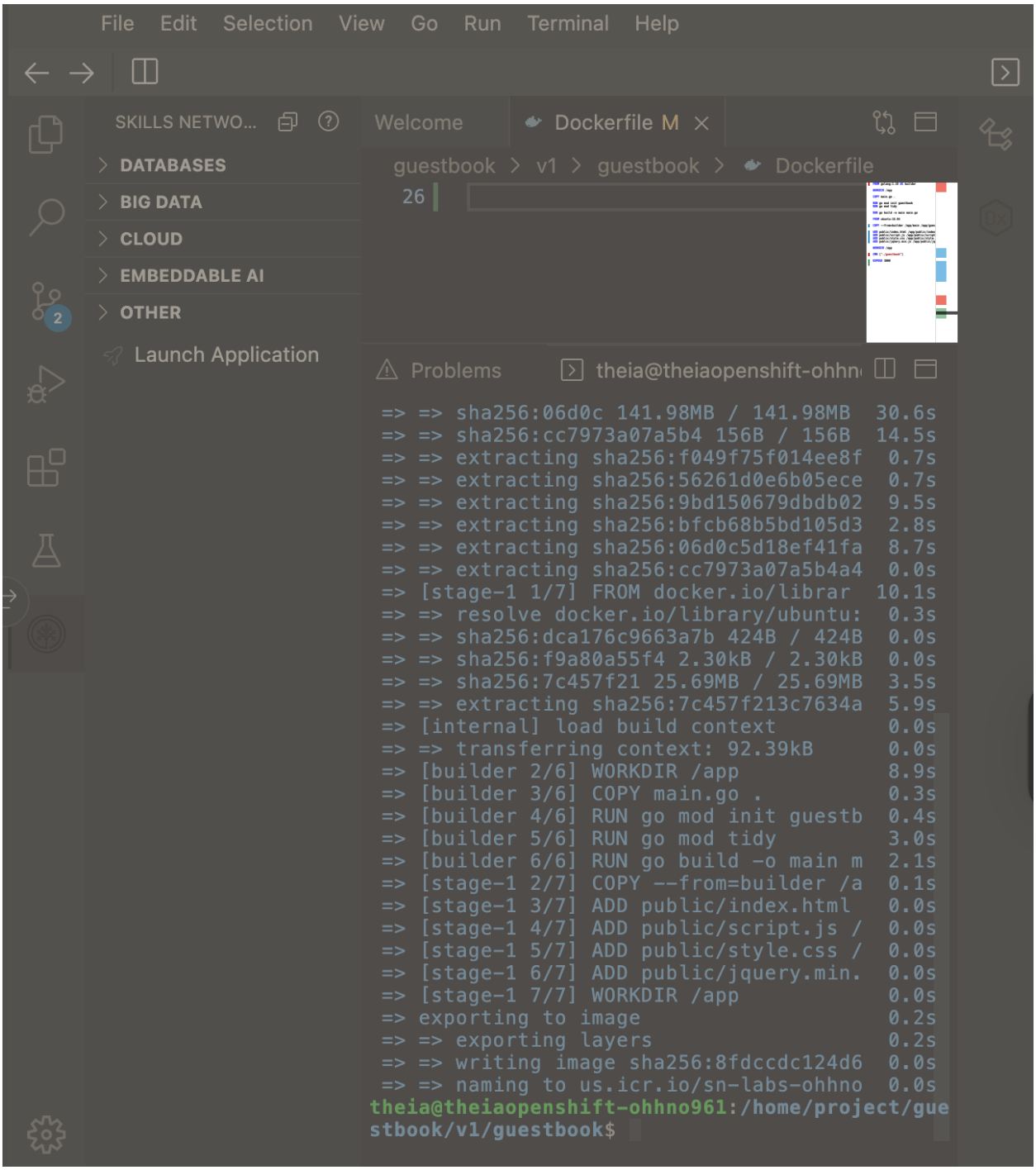
Push (IBM CR):

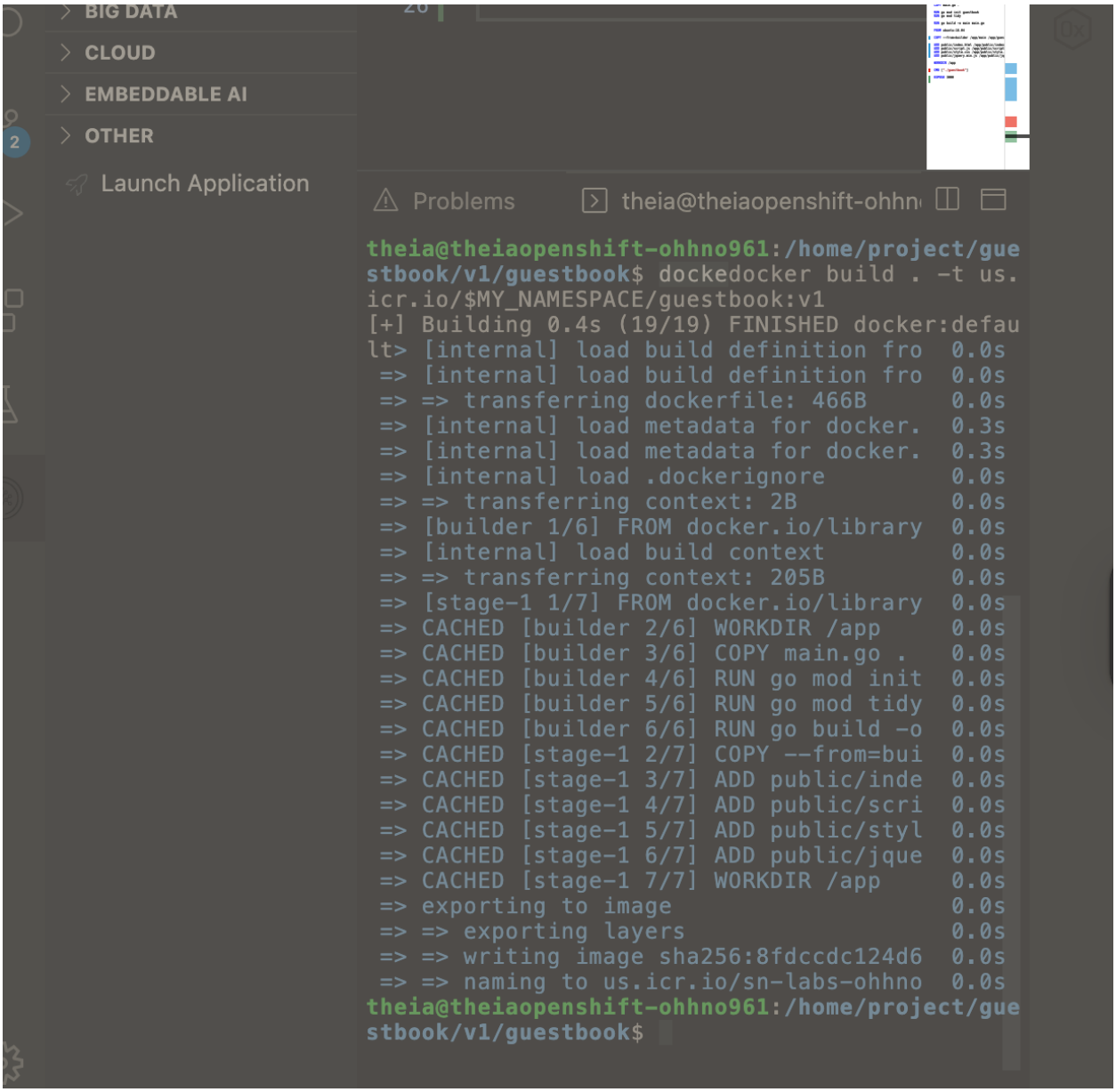
```
bash
# login to IBM Cloud first (lab will have guidance)
# ibmcloud login --apikey $APIKEY
ibmcloud cr login
docker push us.icr.io/${MY_NAMESPACE}/guestbook:v1
# verify
ibmcloud cr images
```

Notes:

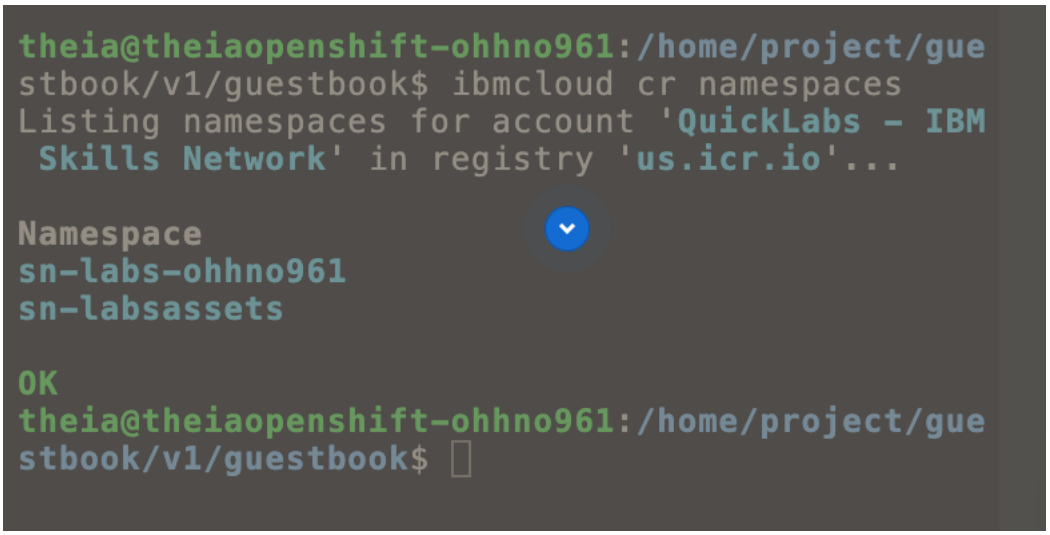
- `imagePullPolicy: Always` in the deployment ensures Kubelet checks registry for newer image versions when a pod is created (see imagePullPolicy docs). Be cautious: `Always` causes image pull attempts and authentication checks on each container start. Kubernetes


File Edit Selection View Go Run Terminal Help
SKILLS NETWO...
DATABASES
BIG DATA
CLOUD
EMBEDDABLE AI
OTHER
Launch Application
Welcome
Dockerfile M
guestbook > v1 > guestbook > Dockerfile
26
Problems
theia@theiaopenshift-ohhn
stbook/v1/guestbook$ export MY_NAMESPACE=sn-lab
s-$USERNAME
theia@theiaopenshift-ohhno961:/home/project/gue
stbook/v1/guestbook$ dockedocker build . -t us.
icr.io/$MY_NAMESPACE/guestbook:v1
[+] Building 19.3s (6/18) docker:default
=> [internal] load build definition fro 0.1s
=> => transferring dockerfile: 466B 0.0s
=> [internal] load metadata for docker. 0.9s
=> [internal] load metadata for docker. 1.6s
=> [internal] load .dockerignore 0.0s
=> => transferring context: 2B 0.0s
=> [builder 1/6] FROM docker.io/librar 17.6s
=> => resolve docker.io/library/golang: 0.3s
=> => sha256:740324e52d 1.80kB / 1.80kB 0.0s
=> => sha256:c37a56a6d6 7.12kB / 7.12kB 0.0s
=> => sha256:bbeef03c 55.03MB / 55.03MB 8.0s
=> => sha256:f049f75f01 5.16MB / 5.16MB 1.4s
=> => sha256:56261d0e 10.88MB / 10.88MB 7.7s
=> => sha256:9bd1506 54.58MB / 54.58MB 12.7s
=> => sha256:bfcb68b 48.23MB / 85.98MB 17.3s
=> => extracting sha256:bbeef03cda1f5d6 9.2s
=> => sha256:06d0c5 50.33MB / 141.98MB 17.3s
=> => sha256:cc7973a07a5b4 156B / 156B 14.5s
=> [stage-1 1/7] FROM docker.io/librar 10.1s
=> => resolve docker.io/library/ubuntu: 0.3s
=> => sha256:dca176c9663a7b 424B / 424B 0.0s
=> => sha256:f9a80a55f4 2.30kB / 2.30kB 0.0s
=> => sha256:7c457f21 25.69MB / 25.69MB 3.5s
=> => extracting sha256:7c457f213c7634a 5.9s
=> [internal] load build context 0.0s
=> => transferring context: 92.39kB 0.0s


File Edit Selection View Go Run Terminal Help
SKILLS NETWO...
Welcome
Dockerfile M
guestbook > v1 > guestbook > Dockerfile
26
DATABASES
BIG DATA
CLOUD
EMBEDDABLE AI
OTHER
Launch Application
Problems
theia@theiaopenshift-ohhn
=> => sha256:06d0c 141.98MB / 141.98MB 30.6s
=> => sha256:cc7973a07a5b4 156B / 156B 14.5s
=> => extracting sha256:f049f75f014ee8f 0.7s
=> => extracting sha256:56261d0e6b05ece 0.7s
=> => extracting sha256:9bd150679dbdb02 9.5s
=> => extracting sha256:bfcb68b5bd105d3 2.8s
=> => extracting sha256:06d0c5d18ef41fa 8.7s
=> => extracting sha256:cc7973a07a5b4a4 0.0s
=> [stage-1 1/7] FROM docker.io/librar 10.1s
=> => resolve docker.io/library/ubuntu: 0.3s
=> => sha256:dca176c9663a7b 424B / 424B 0.0s
=> => sha256:f9a80a55f4 2.30kB / 2.30kB 0.0s
=> => sha256:7c457f21 25.69MB / 25.69MB 3.5s
=> => extracting sha256:7c457f213c7634a 5.9s
=> [internal] load build context 0.0s
=> => transferring context: 92.39kB 0.0s
=> [builder 2/6] WORKDIR /app 8.9s
=> [builder 3/6] COPY main.go . 0.3s
=> [builder 4/6] RUN go mod init guestb 0.4s
=> [builder 5/6] RUN go mod tidy 3.0s
=> [builder 6/6] RUN go build -o main m 2.1s
=> [stage-1 2/7] COPY --from=builder /a 0.1s
=> [stage-1 3/7] ADD public/index.html 0.0s
=> [stage-1 4/7] ADD public/script.js / 0.0s
=> [stage-1 5/7] ADD public/style.css / 0.0s
=> [stage-1 6/7] ADD public/jquery.min. 0.0s
=> [stage-1 7/7] WORKDIR /app 0.0s
=> exporting to image 0.2s
=> => exporting layers 0.2s
=> => writing image sha256:8fdccdc124d6 0.0s
=> => naming to us.icr.io/sn-labs-ohhno 0.0s
theia@theiaopenshift-ohhno961:/home/project/gue
stbook/v1/guestbook$


BIG DATA
CLOUD
EMBEDDABLE AI
OTHER
Launch Application
Problems
theia@theiaopenshift-ohhn
theia@theiaopenshift-ohhno961:/home/project/gue
stbook/v1/guestbook$ dockedocker build . -t us.
icr.io/$MY_NAMESPACE/guestbook:v1
[+] Building 0.4s (19/19) FINISHED docker:defau
lt> [internal] load build definition fro 0.0s
=> [internal] load build definition fro 0.0s
=> => transferring dockerfile: 466B 0.0s
=> [internal] load metadata for docker. 0.3s
=> [internal] load metadata for docker. 0.3s
=> [internal] load .dockerignore 0.0s
=> => transferring context: 2B 0.0s
=> [builder 1/6] FROM docker.io/library 0.0s
=> [internal] load build context 0.0s
=> => transferring context: 205B 0.0s
=> [stage-1 1/7] FROM docker.io/library 0.0s
=> CACHED [builder 2/6] WORKDIR /app 0.0s
=> CACHED [builder 3/6] COPY main.go . 0.0s
=> CACHED [builder 4/6] RUN go mod init 0.0s
=> CACHED [builder 5/6] RUN go mod tidy 0.0s
=> CACHED [builder 6/6] RUN go build -o 0.0s
=> CACHED [stage-1 2/7] COPY --from=bui 0.0s
=> CACHED [stage-1 3/7] ADD public/inde 0.0s
=> CACHED [stage-1 4/7] ADD public/scri 0.0s
=> CACHED [stage-1 5/7] ADD public/styl 0.0s
=> CACHED [stage-1 6/7] ADD public/jque 0.0s
=> CACHED [stage-1 7/7] WORKDIR /app 0.0s
=> exporting to image 0.0s
=> => exporting layers 0.0s
=> => writing image sha256:8fdccdc124d6 0.0s
=> => naming to us.icr.io/sn-labs-ohhno 0.0s
theia@theiaopenshift-ohhno961:/home/project/gue
stbook/v1/guestbook$

```
theia@theiaopenshift-ohhno961:/home/project/guestbook/v1/guestbook$ ibmcloud cr images
Listing images...

Repository                                                  Tag                  Digest          Namespace          Created       Size     Security status
us.icr.io/sn-labs-ohhno961/hello-world                      1                    88edb902ad97    sn-labs-ohhno961   5 hours ago   28 MB    -
us.icr.io/sn-labs-ohhno961/myapp                            v1                   08a2a9dbcbd0    sn-labs-ohhno961   5 hours ago   350 MB   -
us.icr.io/sn-labsassets/categories-watson-nlp-runtime       latest               6b01b1e5527b    sn-labsassets      2 years ago   3.1 GB   -
us.icr.io/sn-labsassets/classification-watson-nlp-runtime   latest               dbd407898549    sn-labsassets      2 years ago   4.0 GB   -
us.icr.io/sn-labsassets/concepts-watson-nlp-runtime         latest               1e4741f10569    sn-labsassets      2 y
```



6 — Kubernetes manifests (recommended & hardened)

Below is the **base** deployment.yml provided in the lab, slightly hardened and extended with liveness/readiness probes, resource requests/limits, securityContext, and imagePullSecrets.

deployment.yml (recommended)

```
yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: guestbook
  labels:
    app: guestbook
spec:
  replicas: 1
  selector:
    matchLabels:
      app: guestbook
  strategy:
    type: RollingUpdate
    rollingUpdate:
      maxSurge: 25%
      maxUnavailable: 25%
  template:
    metadata:
      labels:
        app: guestbook
    spec:
      containers:
      - name: guestbook
        image: us.icr.io/<your-sn-namespace>/guestbook:v1
```

```
        imagePullPolicy: Always
        ports:
        - containerPort: 3000
          name: http
        resources:
          requests:
            cpu: "20m"
            memory: "64Mi"
          limits:
            cpu: "50m"
            memory: "128Mi"
        livenessProbe:
          httpGet:
            path: /health
            port: 3000
          initialDelaySeconds: 15
          periodSeconds: 10
        readinessProbe:
          httpGet:
            path: /
            port: 3000
          initialDelaySeconds: 5
          periodSeconds: 5
        securityContext:
          allowPrivilegeEscalation: false
          readOnlyRootFilesystem: true
          runAsNonRoot: true
      imagePullSecrets:
        - name: ibm-cr-auth  # create if private registry requires
```

service.yml (ClusterIP + sample port-forward)

```
yaml
apiVersion: v1
kind: Service
metadata:
  name: guestbook
spec:
  selector:
    app: guestbook
  ports:
    - protocol: TCP
      port: 3000
      targetPort: 3000
  type: ClusterIP
```

Horizontal Pod Autoscaler (CLI or yaml)

CLI:

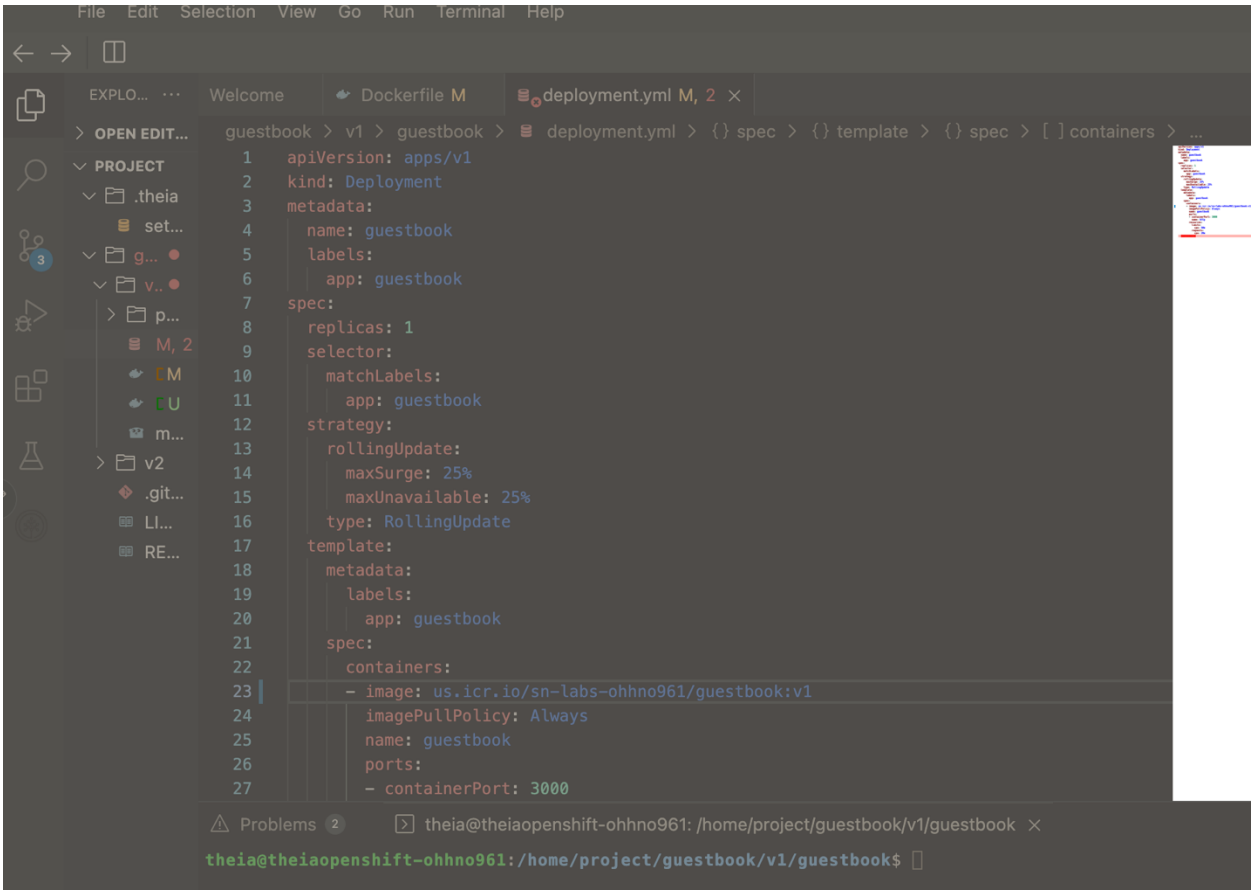
```
bash
kubectl autoscale deployment guestbook --cpu-percent=50 --min=1 --max=10
```

YAML (HPA v2 example using CPU metric):

```
yaml
apiVersion: autoscaling/v2
kind: HorizontalPodAutoscaler
metadata:
  name: guestbook
spec:
  scaleTargetRef:
    apiVersion: apps/v1
    kind: Deployment
    name: guestbook
  minReplicas: 1
  maxReplicas: 10
  metrics:
  - type: Resource
    resource:
      name: cpu
      target:
        type: Utilization
        averageUtilization: 50
```

Notes:

- HPA will only work if a metrics provider (like `metrics-server`) is present. MediumKubernetes
- `rollingUpdate` parameters (`maxSurge` / `maxUnavailable`) control availability vs rollout speed. `maxSurge: 25%` permits extra pods during update; `maxUnavailable: 25%` allows some downtime within that limit. These are critical for safe rollouts. Kubernetesbluematador.com



7 — Deploy, verify, port-forward, smoke test (commands + expected outcomes)

1. Apply manifests:

```
bash
kubectl apply -f deployment.yml
kubectl apply -f service.yml
# or for autoscale:
kubectl autoscale deployment guestbook --cpu-percent=50 --min=1 --max=10
```

2. Verify deployment & pods:

```
bash
kubectl get deploy guestbook
kubectl get pods -l app=guestbook -o wide
kubectl describe deployment guestbook
```

Expected: 1 replica running; `kubectl describe` shows the pod template, image, events.

3. Port-forward to expose the app locally (lab uses port 3000):

```
bash
kubectl port-forward deployment.apps/guestbook 3000:3000
```

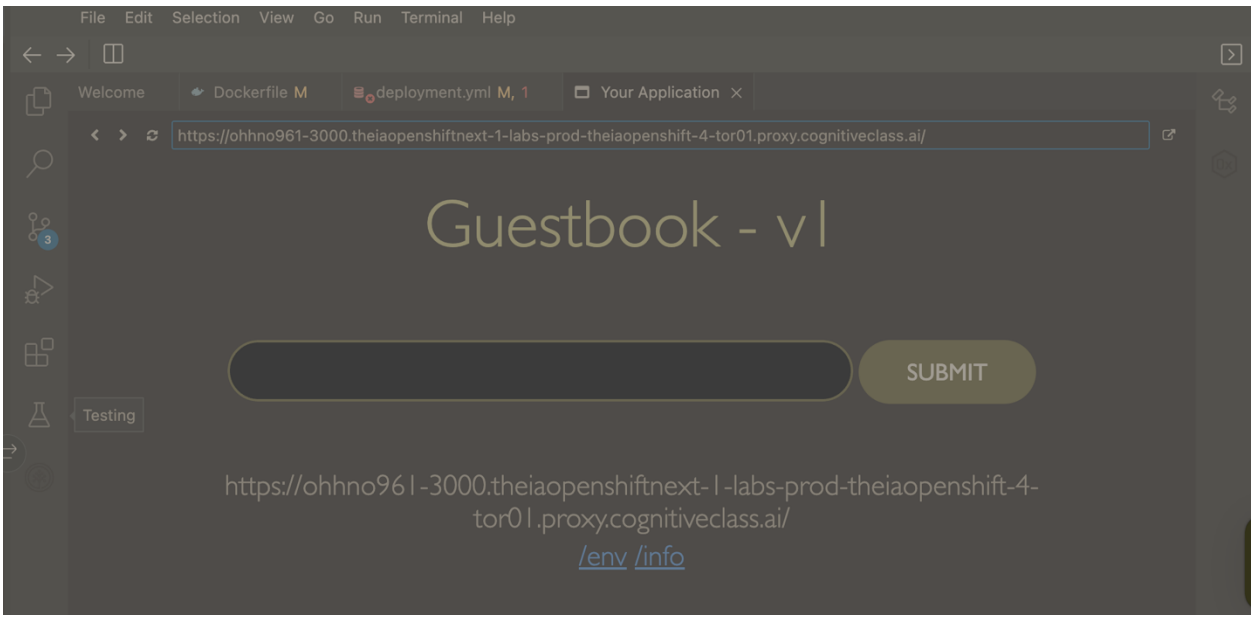
This creates a local tunnel to a selected pod. Use `http://localhost:3000` to access the app. (Docs: port-forward tunnels via the API server.) [Kubernetes]

4. Basic log checks:

```
bash
kubectl logs -l app=guestbook --tail=200
kubectl logs <pod-name> -f
kubectl describe pod <pod-name>
kubectl get events --sort-by='.metadata.creationTimestamp'
```

Smoke test: add entries in the front end and verify they persist (depends on app logic).

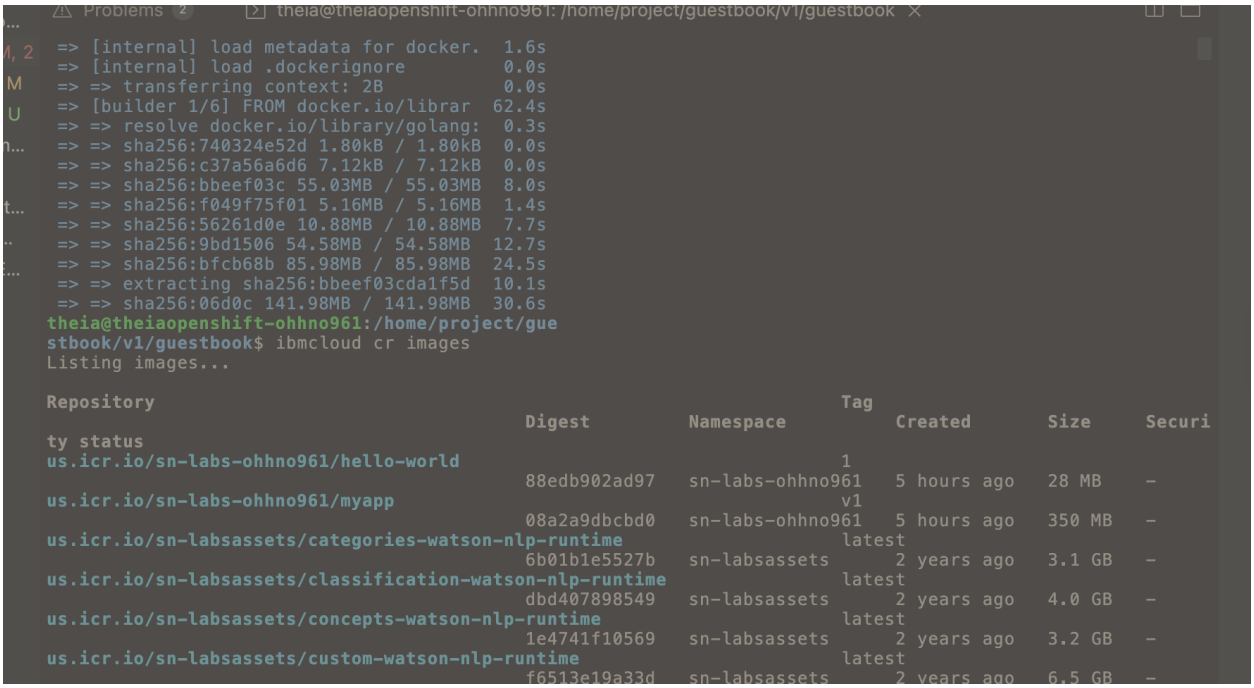
```
theia@theiaopenshift-ohhno961:/home/project/guestbook/v1/guestbook$ docker build -t us.icr.io/sn-labs-ohhno
961/guestbook:v1 .
[+] Building 0.4s (19/19) FINISHED                                                              docker:default
 => [internal] load build definition from Dockerfile                                                     0.0s
 => => transferring dockerfile: 466B                                                                     0.0s
 => [internal] load metadata for docker.io/library/ubuntu:18.04                                          0.3s
 => [internal] load metadata for docker.io/library/golang:1.18                                           0.3s
 => [internal] load .dockerignore                                                                        0.0s
 => => transferring context: 2B                                                                          0.0s
 => [internal] load build context                                                                        0.0s
 => => transferring context: 205B                                                                        0.0s
 => [builder 1/6] FROM docker.io/library/golang:1.18@sha256:740324e52de766f230ad7113fac9028399d6e03a     0.0s
 => [stage-1 1/7] FROM docker.io/library/ubuntu:18.04@sha256:dca176c9663a7ba4c1f0e710986f5a25e672842      0.0s
 => CACHED [builder 2/6] WORKDIR /app                                                                    0.0s
 => CACHED [builder 3/6] COPY main.go .                                                                  0.0s
 => CACHED [builder 4/6] RUN go mod init guestbook                                                       0.0s
 => CACHED [builder 5/6] RUN go mod tidy                                                                 0.0s
 => CACHED [builder 6/6] RUN go build -o main main.go                                                    0.0s
 => CACHED [stage-1 2/7] COPY --from=builder /app/main /app/guestbook                                    0.0s
 => CACHED [stage-1 3/7] ADD public/index.html /app/public/index.html                                    0.0s
 => CACHED [stage-1 4/7] ADD public/script.js /app/public/script.js                                      0.0s
 => CACHED [stage-1 5/7] ADD public/style.css /app/public/style.css                                      0.0s
 => CACHED [stage-1 6/7] ADD public/jquery.min.js /app/public/jquery.min.js                              0.0s
 => CACHED [stage-1 7/7] WORKDIR /app                                                                    0.0s
 => exporting to image                                                                                   0.0s
 => => exporting layers                                                                                  0.0s
 => => writing image sha256:8fdccdc124d633f9ac2e378a2024e9e5ba67b8492d470fb074513e5884951418             0.0s
 => => naming to us.icr.io/sn-labs-ohhno961/guestbook:v1                                                 0.0s
theia@theiaopenshift-ohhno961:/home/project/guestbook/v1/guestbook$
```



```
theia@theiaopenshift-ohhno961:/home/project/guestbook/v1/guestbook$ docker push us.icr.io/sn-labs-ohhno961/
guestbook:v1
The push refers to repository [us.icr.io/sn-labs-ohhno961/guestbook]
5f70bf18a086: Pushed
d33e379b6bf5: Pushed
66d7005838a7: Pushed
10564c280bb3: Pushed
44a241b1145e: Pushed
c8c131370190: Pushed
548a79621a42: Pushed
v1: digest: sha256:ed509938817c14026e636608139299fdf338bf99ba1da37f794c7d1c9c1bc54b size: 1776
theia@theiaopenshift-ohhno961:/home/project/guestbook/v1/guestbook$
```

```
theia@theiaopenshift-ohhno961:/home/project/guestbook/v1/guestbook$ kubectl rollout restart deployment gues
tbook
kubectl get pods
deployment.apps/guestbook restarted
NAME                                    READY   STATUS             RESTARTS   AGE
guestbook-67c998b98d-8cs7w              0/1     ImagePullBackOff   0          2m56s
openshift-web-console-6fc79c9dd5-8st2s  2/2     Running            0          31m
openshift-web-console-6fc79c9dd5-kwrj8  2/2     Running            0          31m
theia@theiaopenshift-ohhno961:/home/project/guestbook/v1/guestbook$
```

```
theia@theiaopenshift-ohhno961:/home/project/guestbook/v1/guestbook$ ibmcloud cr login
Logging 'docker' in to 'us.icr.io'...
Logged in to 'us.icr.io'.

OK
theia@theiaopenshift-ohhno961:/home/project/guestbook/v1/guestbook$ docker push us.icr.io/sn-labs-ohhno961/
guestbook:v1
The push refers to repository [us.icr.io/sn-labs-ohhno961/guestbook]
5f70bf18a086: Layer already exists
d33e379b6bf5: Layer already exists
66d7005838a7: Layer already exists
10564c280bb3: Layer already exists
44a241b1145e: Layer already exists
c8c131370190: Layer already exists
548a79621a42: Layer already exists
v1: digest: sha256:ed509938817c14026e636608139299fdf338bf99ba1da37f794c7d1c9c1bc54b size: 1776
theia@theiaopenshift-ohhno961:/home/project/guestbook/v1/guestbook$
```



```
Problems 2    theia@theiaopenshift-ohhno961: /home/project/guestbook/v1/guestbook
 => [internal] load metadata for docker.  1.6s
 => [internal] load .dockerignore         0.0s
 => => transferring context: 2B           0.0s
 => [builder 1/6] FROM docker.io/librar  62.4s
 => => resolve docker.io/library/golang:  0.3s
 => => sha256:740324e52d 1.80kB / 1.80kB  0.0s
 => => sha256:c37a56a6d6 7.12kB / 7.12kB  0.0s
 => => sha256:bbeef03c 55.03MB / 55.03MB  8.0s
 => => sha256:f049f75f01 5.16MB / 5.16MB  1.4s
 => => sha256:56261d0e 10.88MB / 10.88MB  7.7s
 => => sha256:9bd1506 54.58MB / 54.58MB  12.7s
 => => sha256:bfcb68b 85.98MB / 85.98MB  24.5s
 => => extracting sha256:bbeef03cda1f5d  10.1s
 => => sha256:06d0c 141.98MB / 141.98MB  30.6s
theia@theiaopenshift-ohhno961:/home/project/guestbook/v1/guestbook$ ibmcloud cr images
Listing images...

Repository                                                Tag
                                                  Digest         Namespace          Created       Size     Security status
us.icr.io/sn-labs-ohhno961/hello-world                    1
                                                  88edb902ad97   sn-labs-ohhno961   5 hours ago   28 MB    -
us.icr.io/sn-labs-ohhno961/myapp                          v1
                                                  08a2a9dbcbd0   sn-labs-ohhno961   5 hours ago   350 MB   -
us.icr.io/sn-labsassets/categories-watson-nlp-runtime     latest
                                                  6b01b1e5527b   sn-labsassets      2 years ago   3.1 GB   -
us.icr.io/sn-labsassets/classification-watson-nlp-runtime latest
                                                  dbd407898549   sn-labsassets      2 years ago   4.0 GB   -
us.icr.io/sn-labsassets/concepts-watson-nlp-runtime       latest
                                                  1e4741f10569   sn-labsassets      2 years ago   3.2 GB   -
us.icr.io/sn-labsassets/custom-watson-nlp-runtime         latest
                                                  f6513e19a33d   sn-labsassets      2 years ago   6.5 GB   -
```

```
theia@theiaopenshift-ohhno961:/home/project/guestbook/v1/guestbook$ ibmcloud cr images
Listing images...

Repository                                                Tag
                                                  Digest         Namespace          Created          Size     Security status
us.icr.io/sn-labs-ohhno961/guestbook                      v1
                                                  ed509938817c   sn-labs-ohhno961   10 minutes ago   32 MB    -
us.icr.io/sn-labs-ohhno961/hello-world                    1
                                                  88edb902ad97   sn-labs-ohhno961   6 hours ago      28 MB    -
us.icr.io/sn-labs-ohhno961/myapp                          v1
                                                  08a2a9dbcbd0   sn-labs-ohhno961   5 hours ago      350 MB   -
us.icr.io/sn-labsassets/categories-watson-nlp-runtime     latest
                                                  6b01b1e5527b   sn-labsassets      2 years ago      3.1 GB   -
us.icr.io/sn-labsassets/classification-watson-nlp-runtime latest
                                                  dbd407898549   sn-labsassets      2 years ago      4.0 GB   -
us.icr.io/sn-labsassets/concepts-watson-nlp-runtime       latest
                                                  1e4741f10569   sn-labsassets      2 years ago      3.2 GB   -
us.icr.io/sn-labsassets/custom-watson-nlp-runtime         latest
                                                  f6513e19a33d   sn-labsassets      2 years ago      6.5 GB   -
us.icr.io/sn-labsassets/detag-watson-nlp-runtime          latest
                                                  38916c2119fc   sn-labsassets      2 years ago      2.7 GB   -
us.icr.io/sn-labsassets/emotion-watson-nlp-runtime        latest
                                                  1c9de1d27318   sn-labsassets      2 years ago      4.0 GB   -
us.icr.io/sn-labsassets/entity-mentions-bert-watson-nlp-runtime latest
                                                  57d92957214f   sn-labsassets      2 years ago      3.8 GB   -
us.icr.io/sn-labsassets/entity-mentions-bilstm-watson-nlp-runtime latest
                                                  76dbd3bdb12b   sn-labsassets      2 years ago      2.9 GB   -
us.icr.io/sn-labsassets/entity-mentions-rbr-multi-watson-nlp-runtime latest
                                                  577399d7b4e7   sn-labsassets      2 years ago      2.7 GB   -
us.icr.io/sn-labsassets/entity-mentions-rbr-watson-nlp-runtime latest
                                                  506cc92ecd3f   sn-labsassets      2 years ago      2.7 GB   -
us.icr.io/sn-labsassets/entity-mentions-sire-watson-nlp-runtime latest
```

8 — Autoscaling (HPA) — design, verify, and SOC considerations

How HPA works (short)

HPA periodically reads metrics (CPU by default) from the Metrics API and instructs the Deployment controller to change replica counts to match target utilization. HPA is implemented as an API resource + controller. Kubernetes

Important ops details:

- Default polling cadence and scale cooldown behaviors depend on cluster/provider (AKS docs note HPA checks every 15s for recommendations; scale-down default cooldown is often 5 minutes). HPA scale-events can lag metrics. Microsoft Learn
- HPA alone scales pods; the Cluster Autoscaler or a provider like Karpenter scales nodes (node capacity). Use both for full elasticity. ScaleOps

Verify HPA:

```
bash
kubectl get hpa guestbook
kubectl describe hpa guestbook   # shows current vs target utilization,
events
kubectl get hpa guestbook --watch
```

Expected: HPA shows target (50%) and current average CPU. When under load the HPA will increase desired replicas.

Generate load (lab example)

1. Keep `kubectl port-forward` running to expose the app at `http://127.0.0.1:3000`.
2. On another terminal, run the provided busybox load generator:

```
bash
kubectl run -i --tty load-generator --rm --image=busybox:1.36.0 --
restart=Never -- /bin/sh -c "while sleep 0.01; do wget -q -O- <your app URL>;
done"
```

Replace `<your app URL>` with the port-forwarded URL (e.g., `http://127.0.0.1:3000/`). Monitor HPA with `kubectl get hpa guestbook --watch`.

SOC considerations — HPA as an attack surface

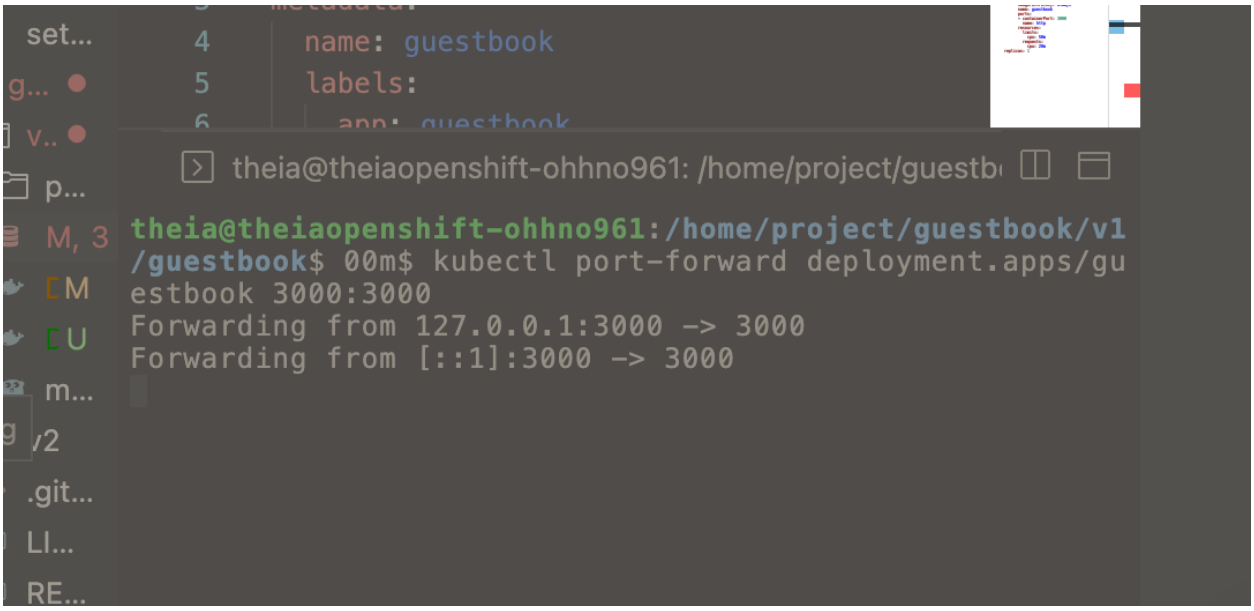
- **Denial-of-Wallet / Economic Denial of Sustainability**: attackers can craft low-volume yet continuous traffic to trigger autoscaling and inflate costs (Yo-Yo attacks / EDoS).

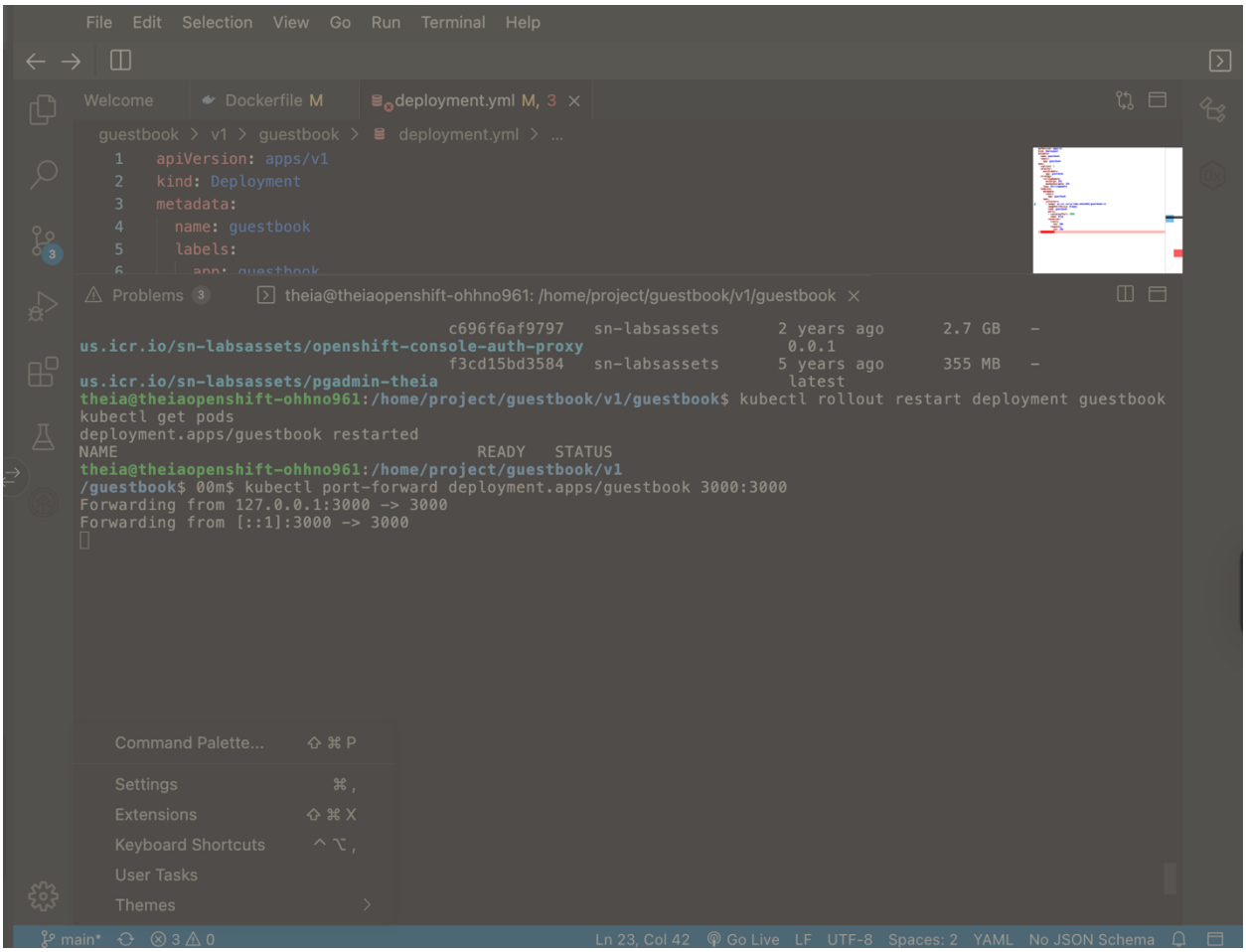
Monitor for recurring scale oscillations and sudden spikes in replica counts that correlate with low-value traffic. Research on autoscaler attacks and mitigation exists — treat autoscaler behavior as a detection surface. [Red Hat Research+1]

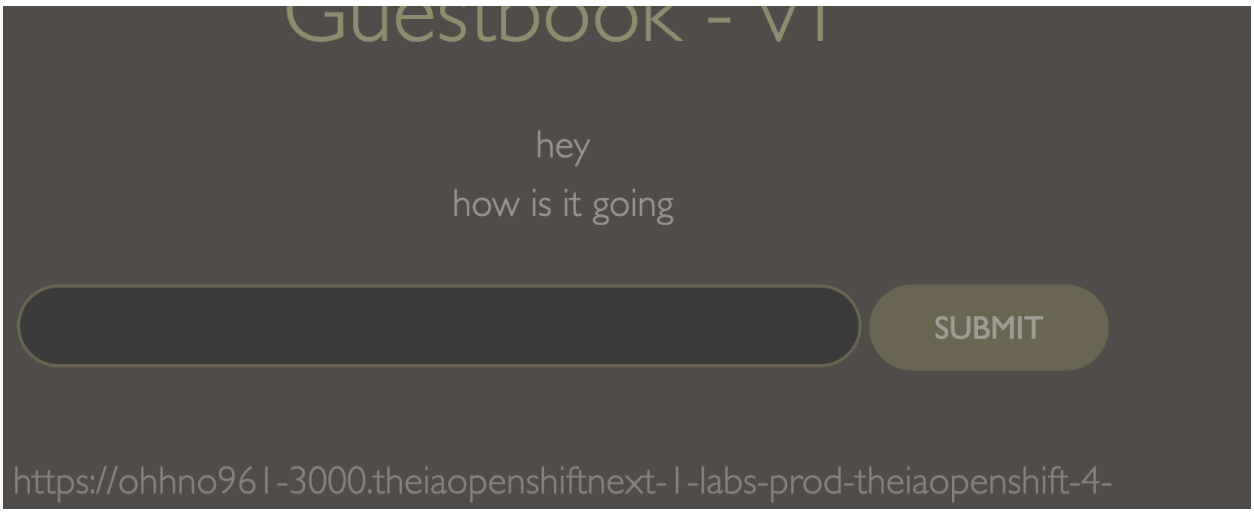
Detections to add (high-level):

- Alerts when HPA increases replicas by >X within Y minutes.
- Alert on repeated scale up/down oscillations (pattern detection).
- Monitor error rates (5xx) and request rates per pod — if HPA scales but error rate rises, suspect inefficient scaling or attack.

```
theia@theiaopenshift-ohhno961:/home/project/guestbook/v1/guestbook$ kubectl rollout restart deployment gues
tbook
kubectl get pods
deployment.apps/guestbook restarted
NAME                                  READY   STATUS    RESTARTS   AGE
guestbook-6c779c48bb-zh5xf            1/1     Running   0          2m15s
openshift-web-console-6fc79c9dd5-8st2s   2/2     Running   0          33m
openshift-web-console-6fc79c9dd5-kwrj8   2/2     Running   0          33m
theia@theiaopenshift-ohhno961:/home/project/guestbook/v1/guestbook$
```



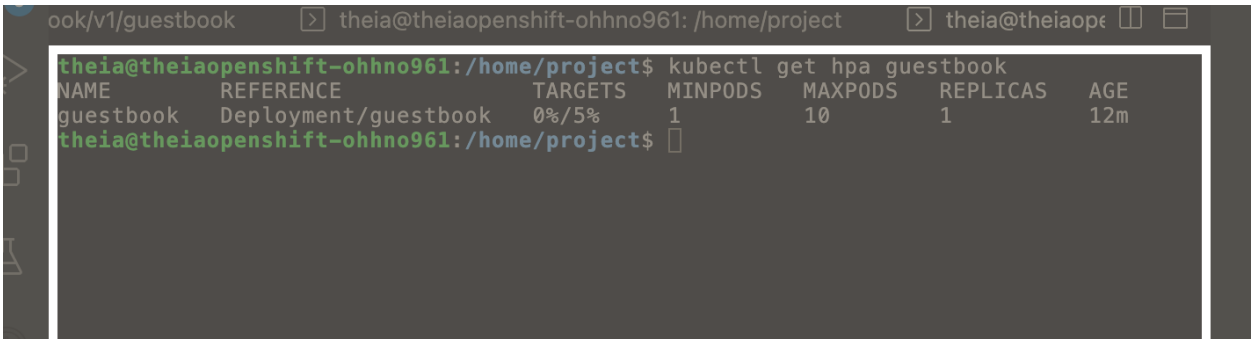

File Edit Selection View Go Run Terminal Help
Welcome
Dockerfile M
deployment.yml M, 3
guestbook > v1 > guestbook > deployment.yml > ...
1 apiVersion: apps/v1
2 kind: Deployment
3 metadata:
4 name: guestbook
5 labels:
Problems 3
theia@theiaopenshift-ohhno961: /home/project/guestbook/v1/guestbook
c696f6af9797 sn-labsassets 2 years ago 2.7 GB -
us.icr.io/sn-labsassets/openshift-console-auth-proxy 0.0.1
f3cd15bd3584 sn-labsassets 5 years ago 355 MB -
us.icr.io/sn-labsassets/pgadmin-theia latest
theia@theiaopenshift-ohhno961:/home/project/guestbook/v1/guestbook$ kubectl rollout restart deployment guestbook
kubectl get pods
deployment.apps/guestbook restarted
NAME READY STATUS
theia@theiaopenshift-ohhno961:/home/project/guestbook/v1
/guestbook$ 00m$ kubectl port-forward deployment.apps/guestbook 3000:3000
Forwarding from 127.0.0.1:3000 -> 3000
Forwarding from [::1]:3000 -> 3000
Command Palette... ⇧ ⌘ P
Settings ⌘ ,
Extensions ⇧ ⌘ X
Keyboard Shortcuts ^ ⌥ ,
User Tasks
Themes
main* ⊗ 3 ⚠ 0
Ln 23, Col 42 Go Live LF UTF-8 Spaces: 2 YAML No JSON Schema

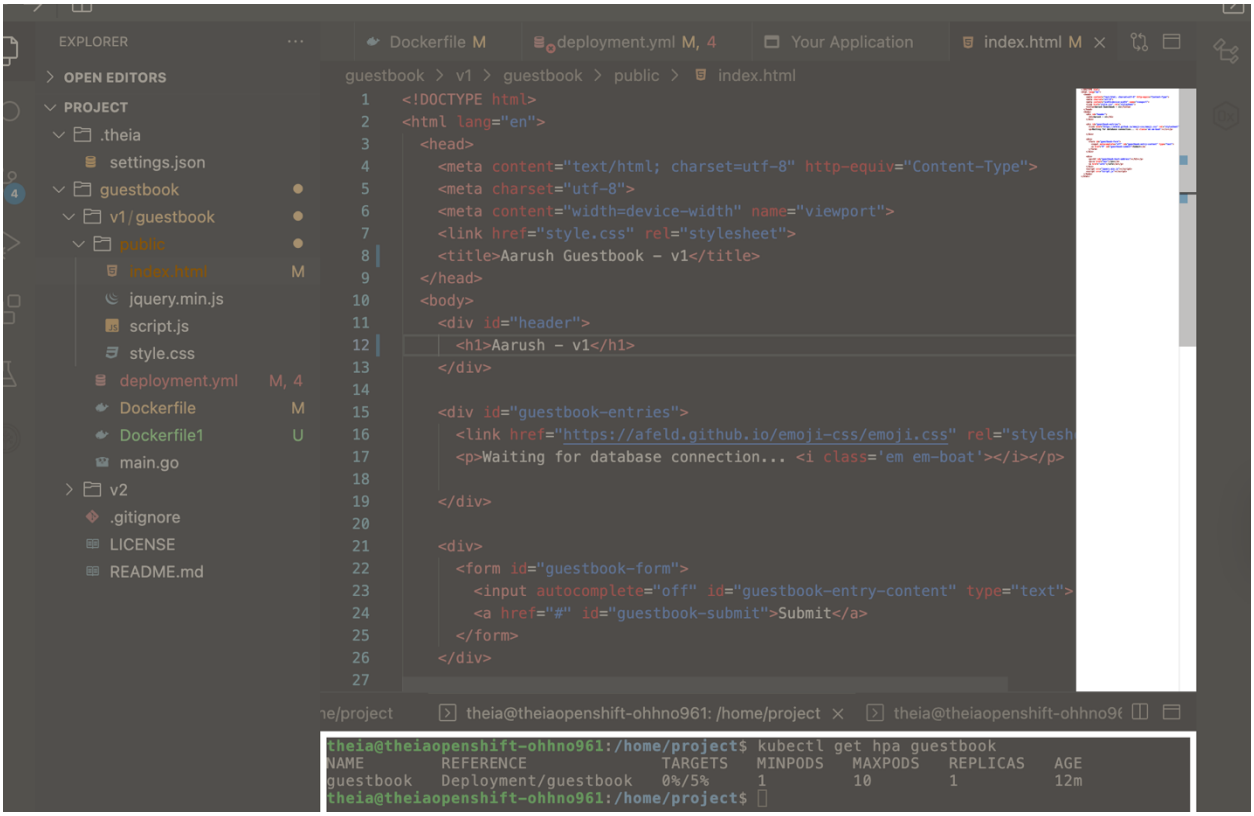

Guestbook - v1
hey
how is it going
SUBMIT
https://ohhno961-3000.theiaopenshiftnext-1-labs-prod-theiaopenshift-4-

```
    <meta content="text/html; charset=utf-8" http-equiv="Content-Type">
    <meta charset="utf-8">
    <meta content="width=device-width" name="viewport">
    <link href="style.css" rel="stylesheet">
    <title>Lavanya's Guestbook - v1</title>
  </head>
  <body>
    <div id="header">
      <h1>Guestbook - v1</h1>
    </div>

    <div id="guestbook-entries">
      <link href="https://afeld.github.io/emoji-css/emoji.css" rel="stylesheet">
      <p>Waiting for database connection... <i class='em em-boat'></i></p>

    </div>

    <div>
      <form id="guestbook-form">
        <input autocomplete="off" id="guestbook-entry-content" type="text">
        <a href="#" id="guestbook-submit">Submit</a>
      </form>
    </div>

    <div>
      <p><h2 id="guestbook-host-address"></h2></p>
      <p><a href="env">/env</a>
      <a href="info">/info</a></p>
    </div>
    <script src="jquery.min.js"></script>
    <script src="script.js"></script>
  </body>
</html>
wget: note: TLS certificate validation not implemented
```

```
theia@theiaopenshift-ohhno961:/home/project$ kubectl get hpa guestbook --watch
NAME        REFERENCE              TARGETS   MINPODS   MAXPODS   REPLICAS   AGE
guestbook   Deployment/guestbook   15%/5%    1         10        3          4m44s
guestbook   Deployment/guestbook   20%/5%    1         10        3          4m47s
guestbook   Deployment/guestbook   20%/5%    1         10        4          5m2s
```

```
theia@theiaopenshift-ohhno961:/home/project$ kubectl get hpa guestbook --watch
NAME        REFERENCE              TARGETS   MINPODS   MAXPODS   REPLICAS   AGE
guestbook   Deployment/guestbook   15%/5%    1         10        3          4m44s
guestbook   Deployment/guestbook   20%/5%    1         10        3          4m47s
guestbook   Deployment/guestbook   20%/5%    1         10        4          5m2s
guestbook   Deployment/guestbook   0%/5%     1         10        4          5m17s
```


ook/v1/guestbook
theia@theiaopenshift-ohhno961: /home/project
theia@theiaope
theia@theiaopenshift-ohhno961:/home/project$ kubectl get hpa guestbook
NAME REFERENCE TARGETS MINPODS MAXPODS REPLICAS AGE
guestbook Deployment/guestbook 0%/5% 1 10 1 12m
theia@theiaopenshift-ohhno961:/home/project$


EXPLORER
OPEN EDITORS
PROJECT
.theia
settings.json
guestbook
v1/guestbook
public
index.html M
jquery.min.js
script.js
style.css
deployment.yml M, 4
Dockerfile M
Dockerfile1 U
main.go
v2
.gitignore
LICENSE
README.md
Dockerfile M
deployment.yml M, 4
Your Application
index.html M
guestbook > v1 > guestbook > public > index.html
<!DOCTYPE html>
<html lang="en">
<head>
<meta content="text/html; charset=utf-8" http-equiv="Content-Type">
<meta charset="utf-8">
<meta content="width=device-width" name="viewport">
<link href="style.css" rel="stylesheet">
<title>Aarush Guestbook - v1</title>
</head>
<body>

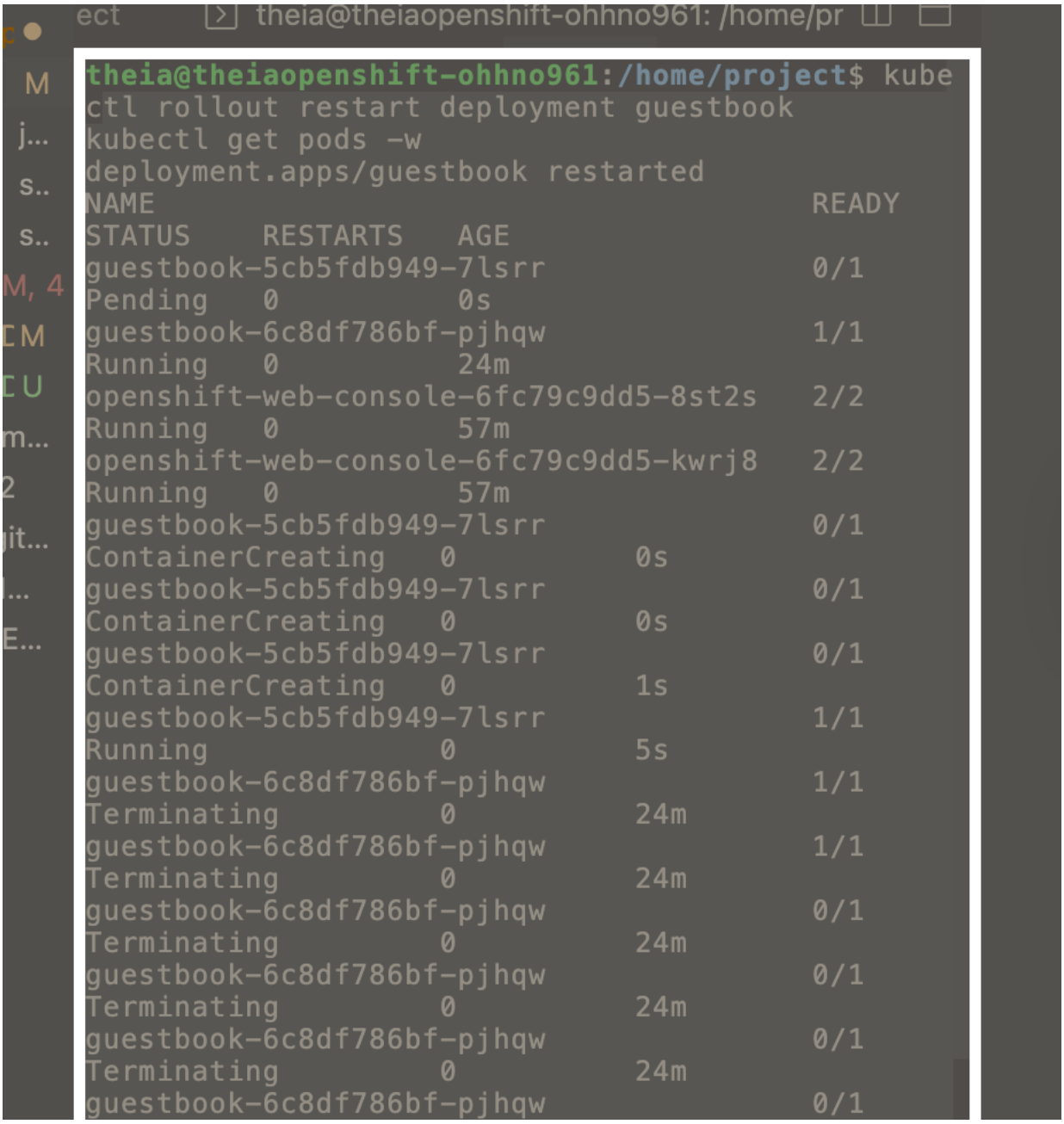
<h1>Aarush - v1</h1>

<link href="https://afeld.github.io/emoji-css/emoji.css" rel="stylesh
Waiting for database connection...

<form id="guestbook-form">
<input autocomplete="off" id="guestbook-entry-content" type="text">
Submit
</form>

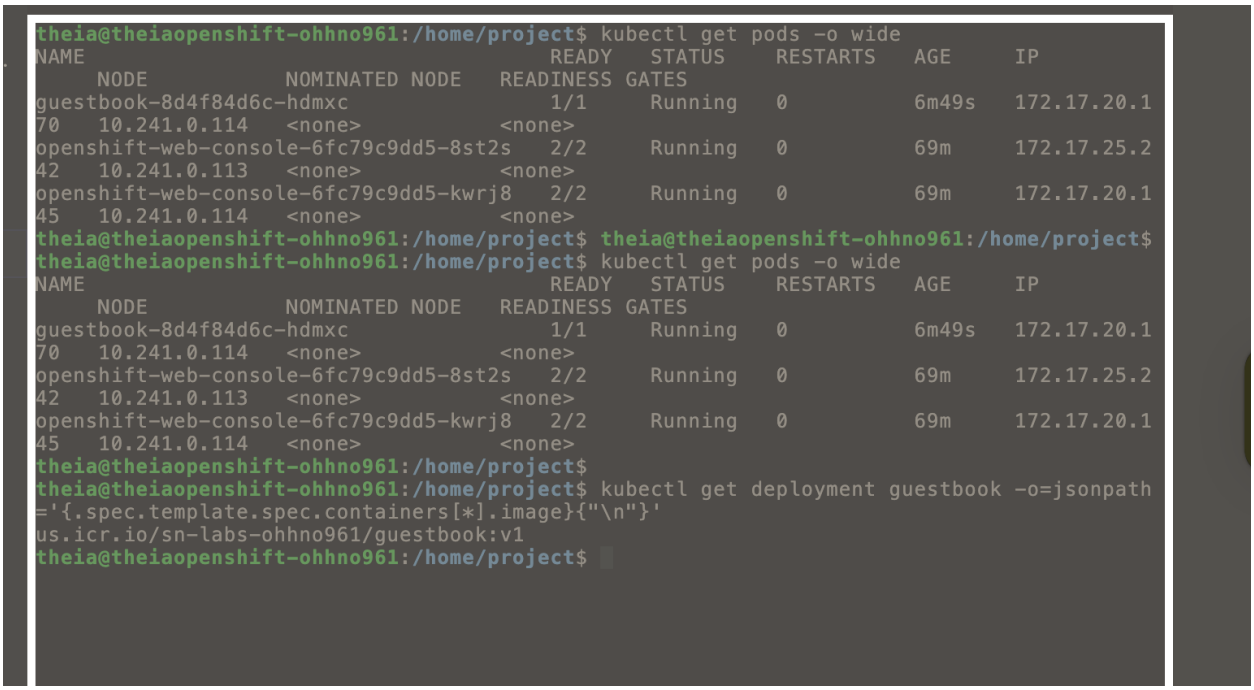
theia@theiaopenshift-ohhno961: /home/project
theia@theiaopenshift-ohhno961:/home/project$ kubectl get hpa guestbook
NAME REFERENCE TARGETS MINPODS MAXPODS REPLICAS AGE
guestbook Deployment/guestbook 0%/5% 1 10 1 12m
theia@theiaopenshift-ohhno961:/home/project$

```
theia@theiaopenshift-ohhno961:/home/project$ expo
rt MY_NAMESPACE=sn-labs-ohhno961
theia@theiaopenshift-ohhno961:/home/project$ dock
er build . -t us.icr.io/$MY_NAMESPACE/guestbook:v
1
docker push us.icr.io/$MY_NAMESPACE/guestbook:v1
[+] Building 0.1s (1/1) FINISHED  docker:default
 => [internal] load build definition from   0.0s
 => => transferring dockerfile: 2B          0.0s
ERROR: failed to solve: failed to read dockerfile
: open Dockerfile: no such file or directory
The push refers to repository [us.icr.io/sn-labs-
ohhno961/guestbook]
5f70bf18a086: Layer already exists
d33e379b6bf5: Layer already exists
66d7005838a7: Layer already exists
10564c280bb3: Layer already exists
44a241b1145e: Layer already exists
c8c131370190: Layer already exists
548a79621a42: Layer already exists
v1: digest: sha256:ed509938817c14026e636608139299
fdf338bf99ba1da37f794c7d1c9c1bc54b size: 1776
theia@theiaopenshift-ohhno961:/home/project$
```


ect
theia@theiaopenshift-ohhno961: /home/pr
theia@theiaopenshift-ohhno961:/home/project$ kube
ctl rollout restart deployment guestbook
kubectl get pods -w
deployment.apps/guestbook restarted
NAME READY
STATUS RESTARTS AGE
guestbook-5cb5fdb949-7lsrr 0/1
Pending 0 0s
guestbook-6c8df786bf-pjhqw 1/1
Running 0 24m
openshift-web-console-6fc79c9dd5-8st2s 2/2
Running 0 57m
openshift-web-console-6fc79c9dd5-kwrj8 2/2
Running 0 57m
guestbook-5cb5fdb949-7lsrr 0/1
ContainerCreating 0 0s
guestbook-5cb5fdb949-7lsrr 0/1
ContainerCreating 0 0s
guestbook-5cb5fdb949-7lsrr 0/1
ContainerCreating 0 1s
guestbook-5cb5fdb949-7lsrr 1/1
Running 0 5s
guestbook-6c8df786bf-pjhqw 1/1
Terminating 0 24m
guestbook-6c8df786bf-pjhqw 1/1
Terminating 0 24m
guestbook-6c8df786bf-pjhqw 0/1
Terminating 0 24m
guestbook-6c8df786bf-pjhqw 0/1
Terminating 0 24m
guestbook-6c8df786bf-pjhqw 0/1
Terminating 0 24m
guestbook-6c8df786bf-pjhqw 0/1

```
theia@theiaopenshift-ohhno961:/home/project$ kubectl apply -f /home/proje
ct/guestbook/v1/guestbook/deployment.yml
deployment.apps/guestbook configured
theia@theiaopenshift-ohhno961:/home/project$
```

```
theia@theiaopenshift-ohhno961:/home/project$ kubectl port-forward deployment.apps/
guestbook 3000:3000
Unable to listen on port 3000: Listeners failed to create with the following error
s: [unable to create listener: Error listen tcp4 127.0.0.1:3000: bind: address alr
eady in use unable to create listener: Error listen tcp6 [::1]:3000: bind: address
 already in use]
error: unable to listen on any of the requested ports: [{3000 3000}]
theia@theiaopenshift-ohhno961:/home/project$ lsof -i :3000
bash: lsof: command not found
theia@theiaopenshift-ohhno961:/home/project$ netstat -tulnp | grep 3000
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
tcp        0      0 127.0.0.1:3000          0.0.0.0:*               LISTEN      23
25/kubectl
tcp6       0      0 ::1:3000                :::*                    LISTEN      23
25/kubectl
theia@theiaopenshift-ohhno961:/home/project$ kill -9 2325
theia@theiaopenshift-ohhno961:/home/project$ kubectl port-forward deployment.apps/
guestbook 3000:3000
Forwarding from 127.0.0.1:3000 -> 3000
Forwarding from [::1]:3000 -> 3000
```



9 — Rolling updates & rollbacks — mechanics + commands

RollingUpdate strategy recap

`spec.strategy.type: RollingUpdate` with `maxSurge` and `maxUnavailable` controls how many extra pods are created and how many can be down during update. This balances speed vs availability. [Kubernetesbluematador.com]

Do an update (two methods)

A — Edit `index.html` to v2, build new image `guestbook:v2`, push to registry, then:

```
bash
kubectl set image deployment/guestbook
guestbook=us.icr.io/${MY_NAMESPACE}/guestbook:v2
kubectl rollout status deployment/guestbook
```

B — Update `deployment.yml` with new image and `kubectl apply -f deployment.yml`.

Check rollout history & revision details:

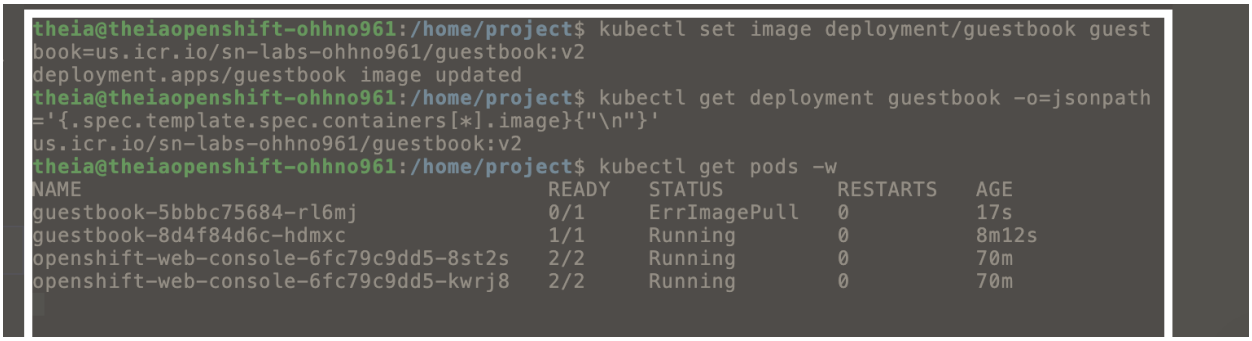
```
bash
kubectl rollout history deployment/guestbook
kubectl rollout history deployment/guestbook --revision=2
kubectl get rs  # shows ReplicaSets and which revision is active
```

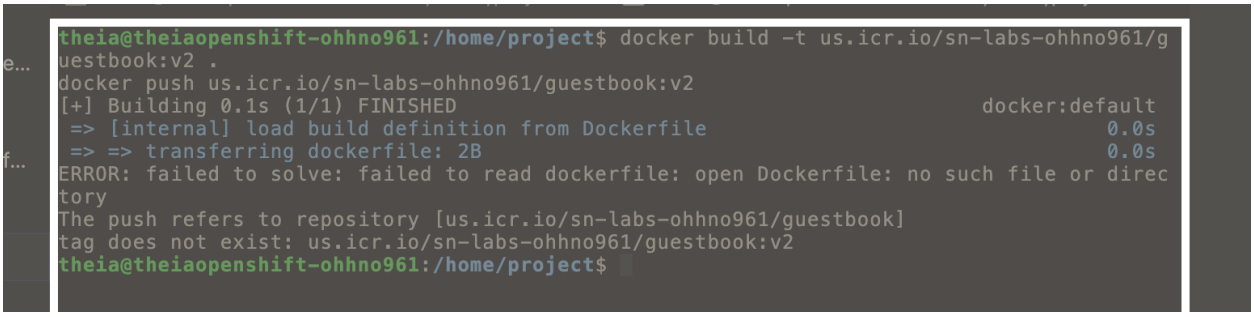
Rollback:

```
bash
kubectl rollout undo deployment/guestbook --to-revision=1
kubectl get rs
```

`rollout undo` switches the deployment spec to a prior ReplicaSet revision. Use `kubectl rollout history` to inspect metadata. Kubernetes

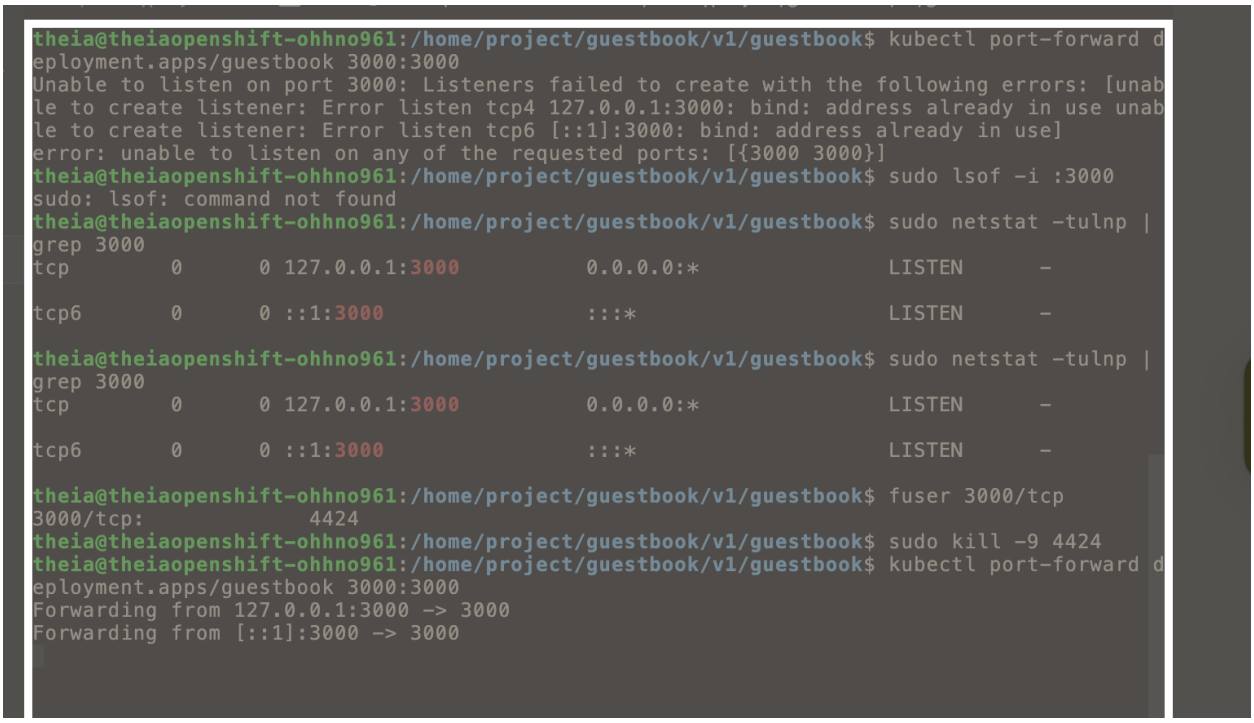
SOC note: **record the exact image digest** for forensic reproducibility (use digest tags `@sha256:...`), not just `:v2`. That avoids tag-repointing issues.

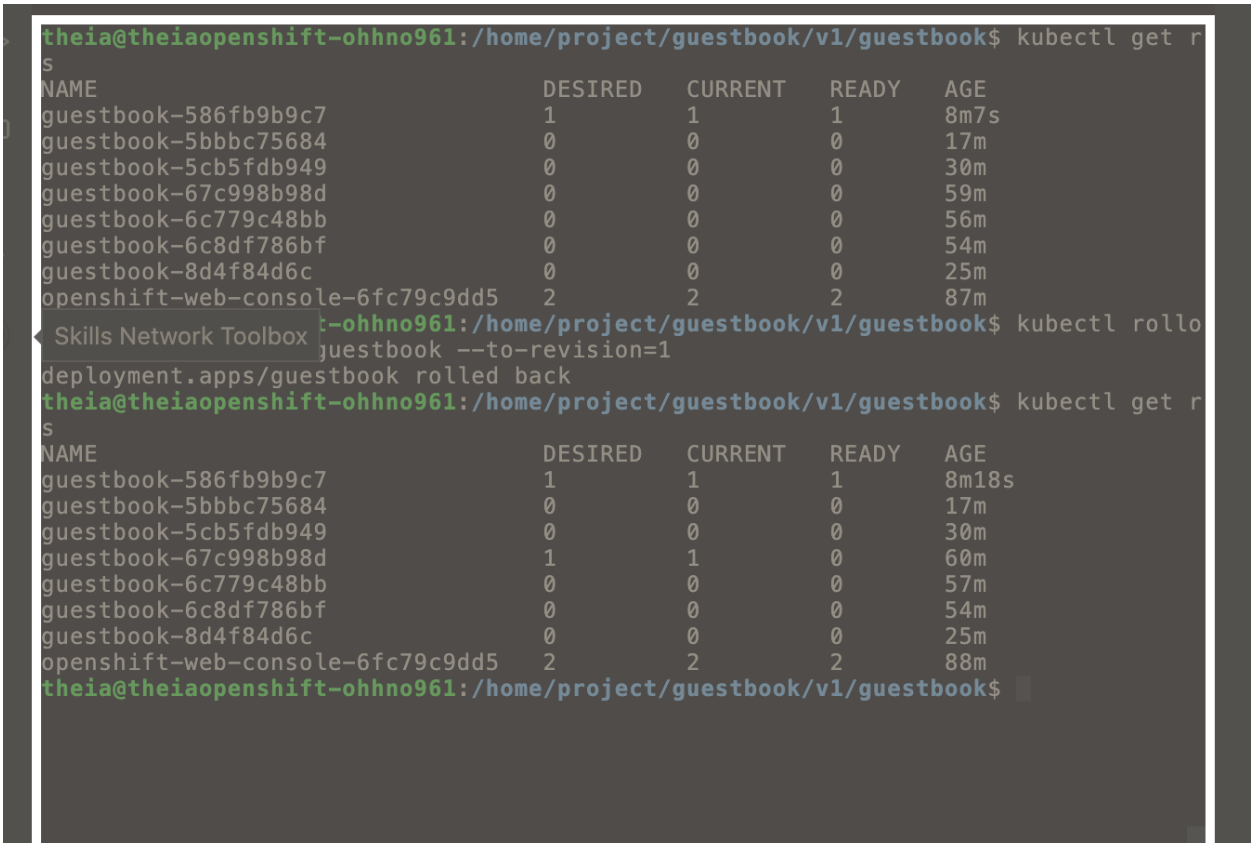




```
theia@theiaopenshift-ohhno961:/home/project$ cd guestbook/v1/guestbook
ls -l
total 24
-rw-r--r-- 1 theia users  427 Aug  8 17:27 Dockerfile
-rw-r--r-- 1 theia users  427 Aug  8 17:28 Dockerfile1
-rw-r--r-- 1 theia users  647 Aug  8 18:21 deployment.yml
-rw-r--r-- 1 theia users 4863 Aug  8 17:21 main.go
drwxr-sr-x 2 theia users 4096 Aug  8 17:21 public
theia@theiaopenshift-ohhno961:/home/project/guestbook/v1/guestbook$ docker build -t us.ic
r.io/sn-labs-ohhno961/guestbook:v2 .
docker push us.icr.io/sn-labs-ohhno961/guestbook:v2
[+] Building 1.3s (19/19) FINISHED                                  docker:default
 => [internal] load build definition from Dockerfile                          0.0s
 => => transferring dockerfile: 466B                                          0.0s
 => [internal] load metadata for docker.io/library/ubuntu:18.04               0.7s
 => [internal] load metadata for docker.io/library/golang:1.18                0.8s
 => [internal] load .dockerignore                                             0.0s
 => => transferring context: 2B                                               0.0s
 => [stage-1 1/7] FROM docker.io/library/ubuntu:18.04@sha256:dca176c9663a7ba4c1f0e  0.0s
 => [builder 1/6] FROM docker.io/library/golang:1.18@sha256:740324e52de766f230ad71  0.0s
 => [internal] load build context                                             0.0s
 => => transferring context: 1.22kB                                           0.0s
 => CACHED [builder 2/6] WORKDIR /app                                         0.0s
 => CACHED [builder 3/6] COPY main.go .                                       0.0s
 => CACHED [builder 4/6] RUN go mod init guestbook                            0.0s
 => CACHED [builder 5/6] RUN go mod tidy                                      0.0s
 => CACHED [builder 6/6] RUN go build -o main main.go                         0.0s
 => CACHED [stage-1 2/7] COPY --from=builder /app/main /app/guestbook         0.0s
 => [stage-1 3/7] ADD public/index.html /app/public/index.html                0.1s
 => [stage-1 4/7] ADD public/script.js /app/public/script.js                  0.1s
 => [stage-1 5/7] ADD public/style.css /app/public/style.css                  0.1s
 => [stage-1 6/7] ADD public/jquery.min.js /app/public/jquery.min.js          0.0s
 => [stage-1 7/7] WORKDIR /app                                                0.0s
 => exporting to image                                                        0.1s
 => => exporting layers                                                       0.1s
```

```
theia@theiaopenshift-ohhno961:/home/project/guestbook/v1/guestbook$ kubectl set image dep
loyment/guestbook guestbook=us.icr.io/sn-labs-ohhno961/guestbook:v2
kubectl rollout restart deployment guestbook
kubectl get pods -w
deployment.apps/guestbook restarted
NAME                                  READY   STATUS             RESTARTS   AGE
guestbook-5bbbc75684-rl6mj            0/1     ImagePullBackOff   0          9m7s
guestbook-8d4f84d6c-hdmxc             1/1     Running            0          17m
openshift-web-console-6fc79c9dd5-8st2s   2/2     Running            0          79m
openshift-web-console-6fc79c9dd5-kwrj8   2/2     Running            0          79m
guestbook-5bbbc75684-rl6mj            0/1     Terminating        0          9m7s
guestbook-5bbbc75684-rl6mj            0/1     Terminating        0          9m7s
guestbook-5bbbc75684-rl6mj            0/1     Terminating        0          9m7s
guestbook-586fb9b9c7-stvxk            0/1     Pending            0          0s
guestbook-586fb9b9c7-stvxk            0/1     Pending            0          0s
guestbook-586fb9b9c7-stvxk            0/1     ContainerCreating   0          0s
guestbook-5bbbc75684-rl6mj            0/1     Terminating        0          9m8s
guestbook-586fb9b9c7-stvxk            0/1     ContainerCreating   0          1s
guestbook-586fb9b9c7-stvxk            0/1     ContainerCreating   0          1s
guestbook-5bbbc75684-rl6mj            0/1     Terminating        0          9m8s
guestbook-5bbbc75684-rl6mj            0/1     Terminating        0          9m9s
guestbook-5bbbc75684-rl6mj            0/1     Terminating        0          9m9s
guestbook-5bbbc75684-rl6mj            0/1     Terminating        0          9m9s
```


theia@theiaopenshift-ohhno961:/home/project/guestbook/v1/guestbook$ kubectl port-forward d
eployment.apps/guestbook 3000:3000
Unable to listen on port 3000: Listeners failed to create with the following errors: [unab
le to create listener: Error listen tcp4 127.0.0.1:3000: bind: address already in use unab
le to create listener: Error listen tcp6 [::1]:3000: bind: address already in use]
error: unable to listen on any of the requested ports: [{3000 3000}]
theia@theiaopenshift-ohhno961:/home/project/guestbook/v1/guestbook$ sudo lsof -i :3000
sudo: lsof: command not found
theia@theiaopenshift-ohhno961:/home/project/guestbook/v1/guestbook$ sudo netstat -tulnp |
grep 3000
tcp 0 0 127.0.0.1:3000 0.0.0.0:* LISTEN -
tcp6 0 0 ::1:3000 :::* LISTEN -
theia@theiaopenshift-ohhno961:/home/project/guestbook/v1/guestbook$ sudo netstat -tulnp |
grep 3000
tcp 0 0 127.0.0.1:3000 0.0.0.0:* LISTEN -
tcp6 0 0 ::1:3000 :::* LISTEN -
theia@theiaopenshift-ohhno961:/home/project/guestbook/v1/guestbook$ fuser 3000/tcp
3000/tcp: 4424
theia@theiaopenshift-ohhno961:/home/project/guestbook/v1/guestbook$ sudo kill -9 4424
theia@theiaopenshift-ohhno961:/home/project/guestbook/v1/guestbook$ kubectl port-forward d
eployment.apps/guestbook 3000:3000
Forwarding from 127.0.0.1:3000 -> 3000
Forwarding from [::1]:3000 -> 3000

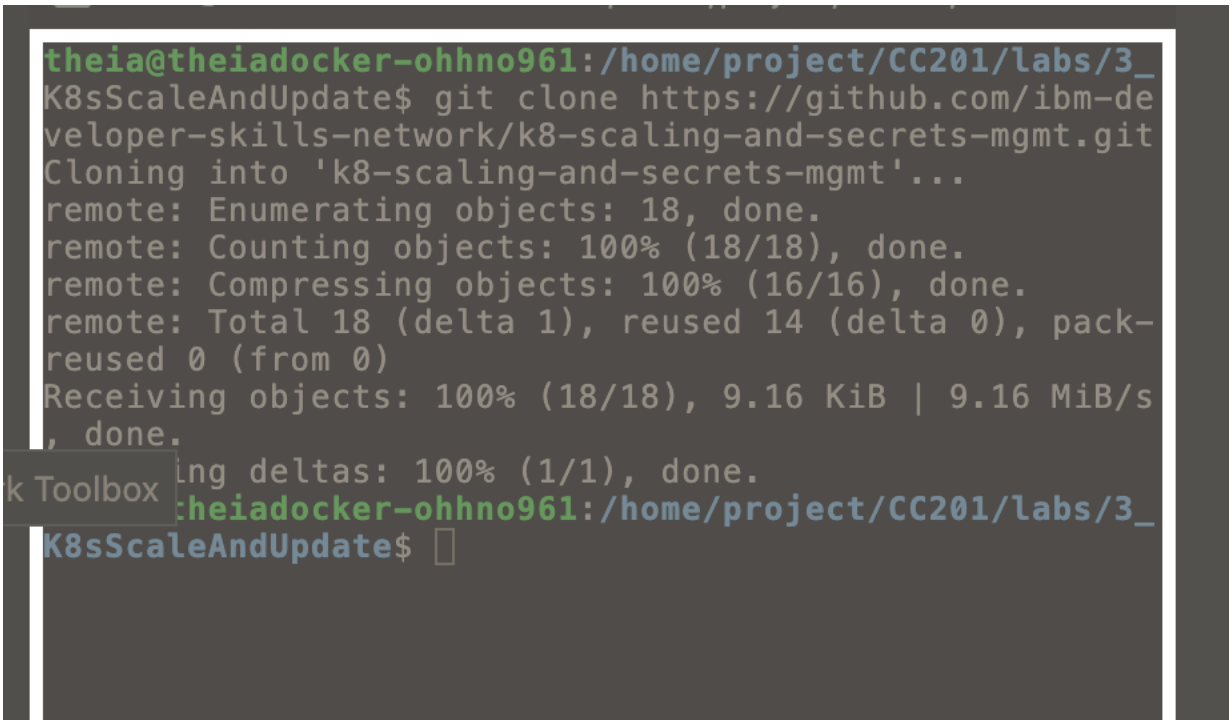

theia@theiaopenshift-ohhno961:/home/project/guestbook/v1/guestbook$ kubectl get r
s
NAME DESIRED CURRENT READY AGE
guestbook-586fb9b9c7 1 1 1 8m7s
guestbook-5bbbc75684 0 0 0 17m
guestbook-5cb5fdb949 0 0 0 30m
guestbook-67c998b98d 0 0 0 59m
guestbook-6c779c48bb 0 0 0 56m
guestbook-6c8df786bf 0 0 0 54m
guestbook-8d4f84d6c 0 0 0 25m
openshift-web-console-6fc79c9dd5 2 2 2 87m
Skills Network Toolbox
-ohhno961:/home/project/guestbook/v1/guestbook$ kubectl rollo
guestbook --to-revision=1
deployment.apps/guestbook rolled back
theia@theiaopenshift-ohhno961:/home/project/guestbook/v1/guestbook$ kubectl get r
s
NAME DESIRED CURRENT READY AGE
guestbook-586fb9b9c7 1 1 1 8m18s
guestbook-5bbbc75684 0 0 0 17m
guestbook-5cb5fdb949 0 0 0 30m
guestbook-67c998b98d 1 1 0 60m
guestbook-6c779c48bb 0 0 0 57m
guestbook-6c8df786bf 0 0 0 54m
guestbook-8d4f84d6c 0 0 0 25m
openshift-web-console-6fc79c9dd5 2 2 2 88m
theia@theiaopenshift-ohhno961:/home/project/guestbook/v1/guestbook$


File Edit Selection View Go Run Terminal Help
Welcome
DATABASES
BIG DATA
CLOUD EMBEDDABLE
OTHER
Launch...
Cloud IDE
Version 1.7.4
VS Code API Version: 1.89.1
Skills Network
What is Cloud IDE?
Cloud IDE is a fully-featured Integrated
Start
New File...
Open
Open Workspace
Recent
theia@theiadocker-ohhno961: /home/project
theia@theiadocker-ohhno961:/home/project$ [! -d 'CC201'] && git clone https://github.com/ibm-developer-skills-network/CC201.git
Cloning into 'CC201'...
remote: Enumerating objects: 30, done.
remote: Counting objects: 100% (7/7), done.
remote: Compressing objects: 100% (7/7), done.
remote: Total 30 (delta 4), reused 0 (delta 0), pack-reused 23 (from 1)
Receiving objects: 100% (30/30), 8.67 KiB | 8.67 MiB/s, done.
Resolving deltas: 100% (13/13), done.
theia@theiadocker-ohhno961:/home/project$

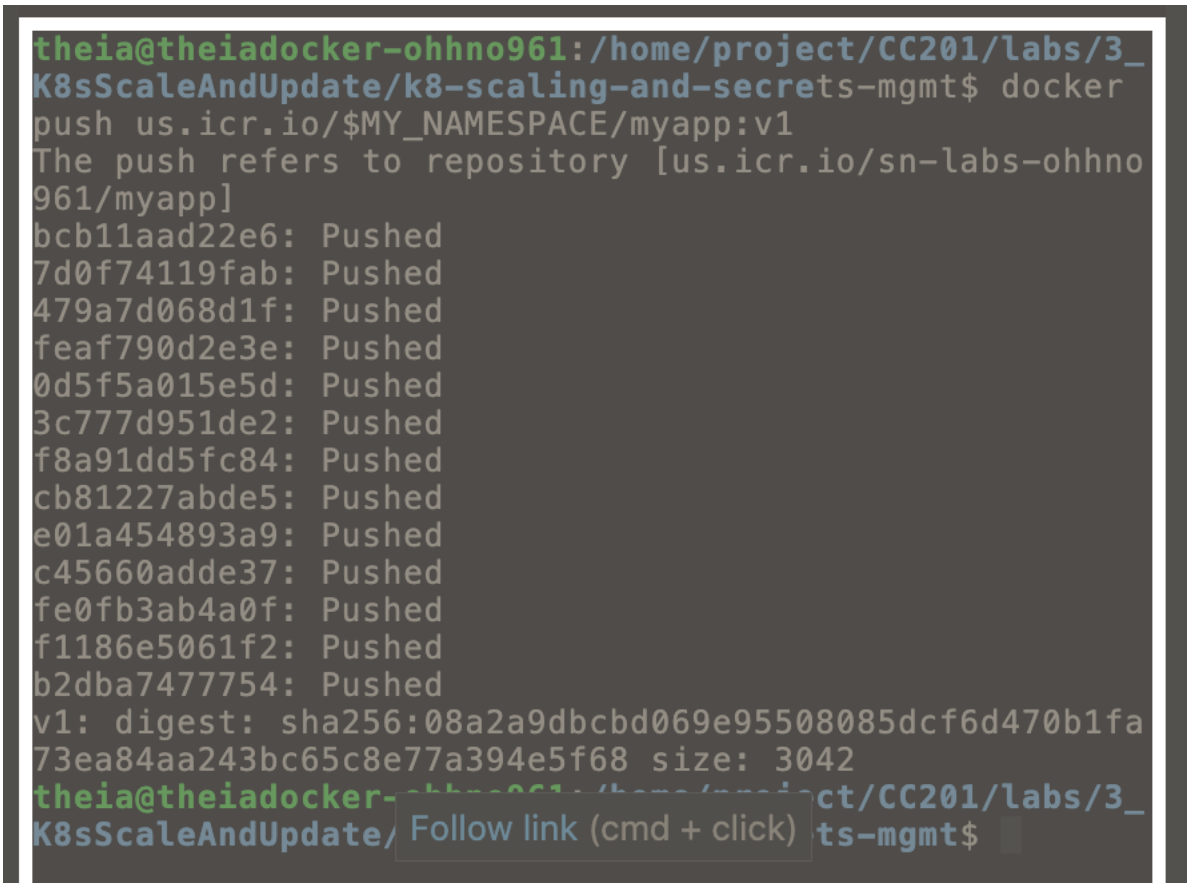
```
theia@theiadocker-ohhno961:/home/project/CC201/labs/3_
K8sScaleAndUpdate$ ls
Dockerfile                          deployment.yaml
app.js                              package.json
deployment-configmap-env-var.yaml
theia@theiadocker-ohhno961:/home/project/CC201/labs/3_
K8sScaleAndUpdate$
```

```
theia@theiadocker-ohhno961:/theia@theiadocker-ohhno961:/home/project/CC201
/labs/3_
K8sScaleAndUpdate$ d    d
ocker build -t us.icr.io/$MY_NAMESPACE/hello-world:1 . && docker push us.i
cr.io/$MY_NAMESPACE/hello-world:1
[+] Building 0.0s (0/0)  doc[+] Building 0.0s (0/1)  doc[+] Building 0.2s
(1/2)  doc[+] Building 0.4s (1/2)  doc[+] Building 0.5s (1/2)  doc[+] Buil
ding 0.7s (1/2)  doc[+] Building 0.8s (1/2)  doc[+] Building 1.0s (1/2)  d
oc[+] Building 1.1s (1/2)  doc[+] Building 1.3s (1/2)  doc[+] Building 1.4
s (1/2)  doc[+] Building 1.6s (1/2)  doc[+] Building 1.7s (1/2)  doc[+] Bu
ilding 1.9s (1/2)  doc[+] Building 2.0s (1/2)  doc[+] Building 2.1s (2/2)
 doc[+] Building 2.3s (4/8)  doc[+] Building 2.5s (4/8)  doc[+] Building 2
.7s (4/8)  doc[+] Buil[+] Building 3.4s (4/8)                 docker:defaul
t
 => [internal] load build definition from Docke  0.1s
 => => transferring dockerfile: 180B             0.0s
 => [internal] load metadata for docker.io/libr  2.0s
```

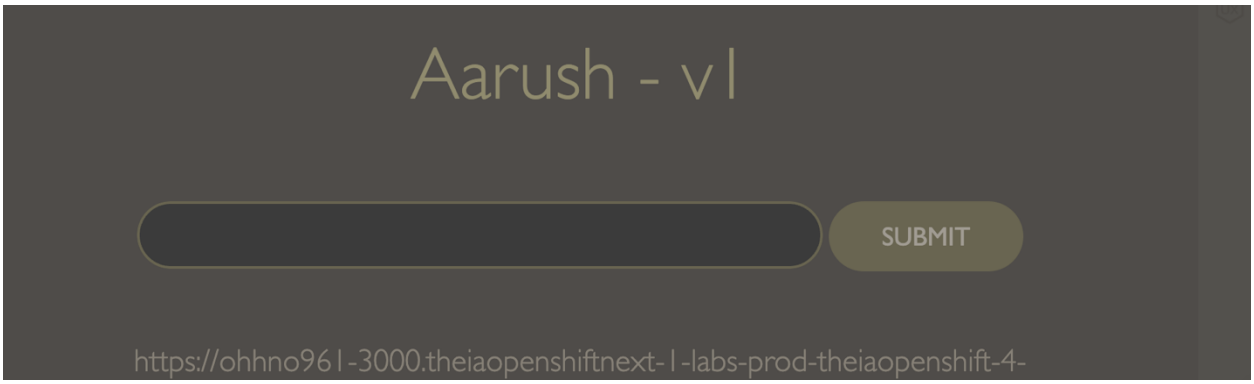
```
 => => transferring context: 2B                                          0.0s
 => [1/4] FROM docker.io/library/node:9.4.0-alpine@sha256:359a2efa4      4.3s
 => => resolve docker.io/library/node:9.4.0-alpine@sha256:359a2efa4      0.0s
 => => sha256:b5f94997f35f4d1ba6221656d90dbe1d9f0ce 4.94kB / 4.94kB      0.0s
 => => sha256:605ce1bd3f3164f2949a30501cc596f52a72d 1.99MB / 1.99MB      0.7s
 => => sha256:fe58b30348fe37cda551e7f3a63375c4697 19.70MB / 19.70MB      1.6s
 => => sha256:46ef8987ccbdd5d2e0127b7eccca7b618fd9b 1.02MB / 1.02MB      0.6s
 => => sha256:359a2efa481b9edeff9ca120128f89387ce13dafe 951B / 951B      0.0s
 => => extracting sha256:605ce1bd3f3164f2949a30501cc596f52a72de05da      0.1s
 => => extracting sha256:fe58b30348fe37cda551e7f3a63375c46977493a48      2.3s
 => => extracting sha256:46ef8987ccbdd5d2e0127b7eccca7b618fd9b17f6a      0.1s
 => [internal] load build context                                        0.0s
 => => transferring context: 574B                                        0.0s
 => [2/4] COPY app.js .                                                  1.3s
 => [3/4] COPY package.json .                                            0.0s
 => [4/4] RUN npm install &&    apk update &&    apk upgrade             3.4s
 => exporting to image                                                   0.3s
 => => exporting layers                                                  0.3s
 => => writing image sha256:835564ebc913cb50f9e795ff26246e5f17832c0      0.0s
 => => naming to us.icr.io/sn-labs-ohhno961/hello-world:1                0.0s

 1 warning found (use docker --debug to expand):
 - JSONArgsRecommended: JSON arguments recommended for CMD to prevent unin
tended behavior related to OS signals (line 8)
The push refers to repository [us.icr.io/sn-labs-ohhno961/hello-world]
eaec4c0b26f7: Pushed
3cfb0d196c00: Pushed
e24f7de2aa49: Pushed
0804854a4553: Pushed
6bd4a62f5178: Pushed
9dfa40a0da3b: Pushed
1: digest: sha256:88edb902ad97fd0f0ed047cad7b14249cd67f589d9125e1e796c4ae6
67695032 size: 1576
theia@theiadocker-ohhno961:/home/project/CC201/labs/3_K8sScaleAndUpdate$
```


theia@theiadocker-ohhno961:/home/project/CC201/labs/3_
K8sScaleAndUpdate$ git clone https://github.com/ibm-de
veloper-skills-network/k8-scaling-and-secrets-mgmt.git
Cloning into 'k8-scaling-and-secrets-mgmt'...
remote: Enumerating objects: 18, done.
remote: Counting objects: 100% (18/18), done.
remote: Compressing objects: 100% (16/16), done.
remote: Total 18 (delta 1), reused 14 (delta 0), pack-
reused 0 (from 0)
Receiving objects: 100% (18/18), 9.16 KiB | 9.16 MiB/s
, done.
ing deltas: 100% (1/1), done.
theiadocker-ohhno961:/home/project/CC201/labs/3_
K8sScaleAndUpdate$
k Toolbox

```
theia@theiadocker-ohhno961:/home/project/CC201/labs/3_
K8sScaleAndUpdate$ cd k8-scaling-and-secrets-mgmt
theia@theiadocker-ohhno961:/home/project/CC201/labs/3_
K8sScaleAndUpdate/k8-scaling-and-secrets-mgmt$ export
MY_NAMESPACE=sn-labs-$USERNAME
theia@theiadocker-ohhno961:/home/project/CC201/labs/3_
K8sScaleAndUpdate/k8-scaling-and-secrets-mgmt$ docker
build . -t us.icr.io/$MY_NAMESPACE/myapp:v1
[+] Building 21.9s (4/9)                    docker:default
 => [internal] load build definition from Docke  0.1s
 => => transferring dockerfile: 464B             0.0s
 => [internal] load metadata for docker.io/libr  1.2s
 => [internal] load .dockerignore                0.0s
 => => transferring context: 2B                  0.0s
 => [1/5] FROM docker.io/library/node:14@sha25  20.5s
 => => resolve docker.io/library/node:14@sha256  0.1s
 => => sha256:1d12470fa662a2a5c 7.51kB / 7.51kB  0.0s
 => => sha256:2ff1d7c41c74a25 50.45MB / 50.45MB  4.8s
 => => sha256:2cafa3fbb0b6529ee 2.21kB / 2.21kB  0.0s
 => => sha256:3d2201bd995cccf 10.00MB / 10.00MB  2.5s
 => => sha256:b253aeafeaa7e0671 7.86MB / 7.86MB  2.3s
 => => sha256:1de76e268b103d0 51.88MB / 51.88MB  9.6s
 => => sha256:d9a8df589451 191.85MB / 191.85MB  20.4s
 => => extracting sha256:2ff1d7c41c74a25258bfa6  7.8s
 => => sha256:6f51ee005deac0d99 4.19kB / 4.19kB  5.4s
 => => sha256:5f32ed3c3f278e 35.24MB / 35.24MB  16.4s
 => => sha256:0c8cc2f24a4dcb64 2.29MB / 2.29MB  12.1s
 => => sha256:0d27a8e861329007574c 450B / 450B  12.8s
 => => extracting sha256:b253aeafeaa7e0671bb600  1.0s
 => => extracting sha256:3d2201bd995cccf12851a5  0.7s
 => => extracting sha256:1de76e268b103d05fa8960  5.1s
 => [internal] load build context                0.1s
 => => transferring context: 2.05kB              0.0s
```


theia@theiadocker-ohhno961:/home/project/CC201/labs/3_K8sScaleAndUpdate/k8-scaling-and-secrets-mgmt$ docker push us.icr.io/$MY_NAMESPACE/myapp:v1
The push refers to repository [us.icr.io/sn-labs-ohhno961/myapp]
bcb11aad22e6: Pushed
7d0f74119fab: Pushed
479a7d068d1f: Pushed
feaf790d2e3e: Pushed
0d5f5a015e5d: Pushed
3c777d951de2: Pushed
f8a91dd5fc84: Pushed
cb81227abde5: Pushed
e01a454893a9: Pushed
c45660adde37: Pushed
fe0fb3ab4a0f: Pushed
f1186e5061f2: Pushed
b2dba7477754: Pushed
v1: digest: sha256:08a2a9dbcbd069e95508085dcf6d470b1fa73ea84aa243bc65c8e77a394e5f68 size: 3042
Follow link (cmd + click)

```
theia@theiadocker-ohhno961:/home/project/CC201/labs/3_
K8sScaleAndUpdate/k8-scaling-and-secrets-mgmt$ ibmclou
d cr images
Listing images...

Repository
                    Tag
                                                    Digest
    Namespace           Created           Size      Secur
ity status
us.icr.io/sn-labs-ohhno961/hello-world
                    1
                                                    88edb902ad9
7   sn-labs-ohhno961    18 minutes ago    28 MB     -
us.icr.io/sn-labs-ohhno961/myapp
                    v1
                                                    08a2a9dbcbd
0   sn-labs-ohhno961    1 minute ago      350 MB    -
us.icr.io/sn-labsassets/categories-watson-nlp-runtime
                    latest
                                                    6b01b1e5527
b   sn-labsassets       2 years ago       3.1 GB    -
us.icr.io/sn-labsassets/classification-watson-nlp-runt
ime                 latest
                                                    dbd40789854
9   sn-labsassets       2 years ago       4.0 GB    -
us.icr.io/sn-labsassets/concepts-watson-nlp-runtime
                    latest
                                                    1e4741f1056
9   sn-labsassets       2 years ago       3.2 GB    -
us.icr.io/sn-labsassets/custom-watson-nlp-runtime
                    latest
                                                    f6513e19a33
d   sn-labsassets       2 years ago       6.5 GB    -
```




```
theia@theiaopenshift-ohhno961:/home/project$ kube
ctl rollout restart deployment guestbook
kubectl get pods -w
deployment.apps/guestbook restarted
NAME                                   READY
STATUS    RESTARTS   AGE
guestbook-5cb5fdb949-7lsrr             0/1
Pending   0          0s
guestbook-6c8df786bf-pjhqw             1/1
Running   0          24m
openshift-web-console-6fc79c9dd5-8st2s   2/2
Running   0          57m
openshift-web-console-6fc79c9dd5-kwrj8   2/2
Running   0          57m
guestbook-5cb5fdb949-7lsrr             0/1
ContainerCreating   0          0s
guestbook-5cb5fdb949-7lsrr             0/1
ContainerCreating   0          0s
guestbook-5cb5fdb949-7lsrr             0/1
ContainerCreating   0          1s
guestbook-5cb5fdb949-7lsrr             1/1
Running             0          5s
guestbook-6c8df786bf-pjhqw             1/1
Terminating         0          24m
guestbook-6c8df786bf-pjhqw             1/1
Terminating         0          24m
guestbook-6c8df786bf-pjhqw             0/1
Terminating         0          24m
guestbook-6c8df786bf-pjhqw             0/1
Terminating         0          24m
```

10 — Observability & logging — what to collect and why (SOC focus)

Telemetry priorities (in order for an incident):

1. **Kubernetes audit logs** (who did what via API — `kubectl`, REST calls). Vital for attributing actions (creates/execs/cronjobs). Ensure audit logging enabled and forwarded. Prisma Cloud Documentationresearch.splunk.com
2. **Pod stdout/stderr** (app logs) aggregated by Fluentd/Fluent Bit / Splunk Connect. Correlate request IDs and errors. Splunk
3. **Kube-controller / kube-scheduler / kube-apiserver logs** (control plane) — for control activities and admission events.
4. **Node syslogs + container runtime logs** (containerd, docker) — to detect process execs, image pulls, local filesystem access.
5. **Falco or eBPF runtime alerts** — detect reverse shells, suspicious file reads (e.g., `/etc/shadow`), privilege escalation attempts. Falco is recommended for real-time detection. Sysdigfalcosecurity.github.io
6. **Metrics (CPU, mem, request rate)** — required for HPA and anomaly detection. HPA needs metrics-server. Medium

Useful `kubectl` commands for telemetry collection

```
bash
kubectl get events -A
kubectl -n <ns> get pods -o wide
kubectl -n <ns> logs <pod> --since=1h
kubectl -n <ns> exec -it <pod> -- sh   # if investigating (but preserve
evidence)
kubectl cp <pod>:/path/to/file /tmp/artifact
kubectl describe hpa guestbook
kubectl describe deployment guestbook
```

Note: For forensics, avoid running `exec` commands that may modify evidence. Prefer `kubectl cp` to retrieve files and `kubectl logs --timestamps` for original timestamps.

11 — Detections & SIEM content (Splunk + Falco examples)

Important: your cluster log schema will vary. These queries are *templates* to adapt to your event fields. Use them in Splunk (index names and field names will vary).

A. Detect creation of privileged pods (Kubernetes audit logs — Splunk)

Splunk has defenses for this — use Kubernetes Audit source to detect privileged pods. Example (conceptual):

```
spl
index=k8s_audit event.verb=create OR event.verb=update
objectRef.resource=pods
| spath input=requestObject.spec.containers{} output=containers
| search requestObject.spec.containers{}.securityContext.privileged=true OR
requestObject.spec.containers{}.securityContext.runAsNonRoot=false
```

(Adapt field names to your ingestion schema.) Splunk has prebuilt analytic detections for "Create or Update Privileged Pod". [research.splunk.com+1]

B. Detect kubectl exec usage (audit)

```
spl
index=k8s_audit verb="create" requestURI="*/exec*"
| stats count by user.username, objectRef.name, requestURI, sourceIPs, _time
| where count > 0
```

Use this to detect interactive shells spawned via `kubectl exec`. Note: does not capture internal commands after exec — Falco complements this. [Splunk CommunitySysdig Docs]

C. Detect unusual image pulls (new registry or many pulls)

```
spl
index=container_runtime_logs action="pull"
| stats count by image, registry, node
| where count > 20
```

Alert if an unusual registry or mass pulls from many nodes occur.

D. Detect HPA rapid scaling / Yo-Yo pattern

```
spl
index=k8s_events kind=HorizontalPodAutoscaler name=guestbook
| timechart span=1m avg(desiredReplicas) as desiredReplicas
| detect_oscillation(desiredReplicas)   # pseudo-function: build logic for
oscillation detection
```

(Implement oscillation detection: sudden repeated changes up & down within small window). Google/Cloud vendor docs show HPA decision logging is emitted; you can add alerts on sudden replica changes. [Google Cloud]

E. Falco runtime rules (examples)

Falco has built-in rules such as:

- Detect shell spawned inside container (possible reverse shell).
- Detect new outbound SSH / unusual network connections from container.
- Detect sensitive file access (e.g., `/etc/shadow`) from container.
  Falco rules are ready out-of-the-box and can be tuned to reduce noise. Use Falco to send alerts into Splunk (via Falcosidekick). falcosecurity.github.ioFalco

Example Falco rule (simplified)

```
yaml
- rule: Shell Spawned In Container
  desc: Detect a shell such as bash opened inside a container
  condition: container and proc.name in (bash, sh) and not proc.args contains
"kubectl exec"
  output: "Shell spawned in container (user=%user.name
container=%container.id proc=%proc.name cmd=%proc.cmdline)"
  priority: WARNING
```

---

12 — Threat model & MITRE ATT&CK mapping

Public-facing web app → exposed to the Internet. Primary risks:

- **Initial access**: Exploit of vulnerable application (RCE), credential stuffing.
- **Execution & Persistence**: Attacker may spawn shells, create CronJobs, or deploy new workloads.
- **Privilege escalation**: Running containers as root or privileged → node escape.
- **Credential compromise**: Read mounted service account tokens, cloud credentials.
- **Lateral movement & impact**: Use cluster admin bindings to access other namespaces or cloud resources.

Map to MITRE ATT&CK (Containers matrix): see the official containers matrix for techniques & IDs (use for SOC mapping and detection coverage). Example mapping:

- Initial Access: Exploit Public-Facing App (Containers) — ATT&CK Containers matrix. MITRE ATT&CK
- Persistence: Container Orchestration Jobs (CronJob abuse) — T1053.007. MITRE ATT&CK
- Privilege Escalation / Defense Evasion: Privileged containers, hostPath mounts. Madhu Akula

Use the MITRE container matrix to build prioritized detections and gap analysis. MITRE ATT&CK

---

13 — Incident response / Tier-3 runbook (containment → recovery)

This is a concise, actionable playbook a Tier-3 SOC should follow when an alarm indicates a possible compromise (e.g., Falco reverse shell + anomalous image pull + HPA yo-yo).

0) Triage quickly (first 10 minutes)

- Correlate alerts: Falco + Splunk audit + HPA scale events + app logs. Pull the correlated timeline.
- Record IDs, times, user principals, and image digests.

1) Containment (quick, reversible)

- **Scale Deployment to zero** (stops attackers inside pods but preserves cluster objects):

  ```
  bash
  kubectl scale deployment guestbook --replicas=0
  ```

- **Or** patch Deployment to `imagePullPolicy: Never` temporarily and scale to desired safe state (less common).
- **If suspect admin user**: rotate cluster credentials; revoke tokens for compromised accounts (cloud provider IAM).

2) Evidence collection (preserve)

- Collect Pod logs:

  ```
  bash
  kubectl logs <pod> --timestamps --since=24h > pod-logs.txt
  ```

- Copy suspicious files from pod (do **not** run commands that modify evidence):

  ```
  bash
  kubectl cp <pod>:/path/to/file ./evidence/
  ```

- Export kube audit logs, apiserver logs, node syslogs, containerd logs.

3) Forensics on nodes (if pod escape suspected)

- Evacuate node (cordon + drain) and create VM snapshot for forensic imaging:

  ```
  bash
  kubectl cordon <node>
  kubectl drain <node> --ignore-daemonsets --delete-local-data
  ```

- Use provider snapshot for disk capture (cloud console).

4) Eradication & recovery

- Replace images with scanned (fixed) images referenced by digest `@sha256:...`; redeploy.
- Reset any exposed secrets and rotate keys (service account tokens, cloud IAM keys).
- Rebuild nodes if host compromise is confirmed.

5) Post-incident: root cause & preventive

- Fix vulnerable app or library (CVEs), update CI to block high-severity images, deploy Pod Security Admission / Gatekeeper / Kyverno policies, enable stricter PSS (baseline or restricted).
- Restore from known good images, confirm absence of backdoors.

(Use MITRE mapping in Section 12 to classify the attacker tactics during the post-incident analysis.)

---

14 — Hardening checklist & continuous controls (priority order)

1. **Image pipeline**
   - Mandatory image scanning in CI (Trivy / Clair / Anchore). Fail build on criticals. aquasecurity.github.iotrivy.dev
   - Use immutable digests for production images (`image@sha256:...`), not `:latest`.
   - Minimal base images; dependency pinning.
2. **Kubernetes control plane & cluster**
   - Apply Pod Security Standards (PSS) labels to namespaces: enforce `baseline` or `restricted` for production. Kubernetes+1
   - Enforce admission policies via Gatekeeper / Kyverno to block privileged containers. Amazon Web Services, Inc.
   - Least-privilege RBAC: no `cluster-admin` for apps.
   - Enable audit logs and forward to SIEM (audit policy tuned to avoid noise).
3. **Runtime**
   - Deploy Falco (or equivalent) for syscall-level alerts; forward alerts to SIEM and PagerDuty. FalcoSysdig
   - Node hardening, CIS Kubernetes Benchmark checks (CIS guide). CIS
4. **Monitoring & cost controls**
   - Alerts for HPA oscillations and sudden replica spikes (Denial-of-Wallet risk). Red Hat Research
   - Budget/alerting at cloud billing level to detect unexpected spend.

---

15 — Troubleshooting & common errors (with root causes + fixes)

HPA not scaling

- Likely cause: metrics-server not installed or misconfigured. Check `kubectl get --raw "/apis/metrics.k8s.io/v1beta1/nodes"`. Install metrics-server if missing.

ImagePullBackOff / ErrImagePull

- Cause: wrong registry credentials or image name. Check secret `imagePullSecrets`, `ibmcloud cr images` to verify push succeeded.

Port-forward fails / nothing on 3000

- Check `kubectl get pods` and ensure pods are `Ready`. Confirm containerPort is 3000 and container is listening (liveness/readiness probe passing). `kubectl port-forward` chooses one pod automatically if multiple; specify pod name if ambiguous.

Rollout stuck / maxUnavailable too low

- If `maxUnavailable` prevents new pods from being scheduled (e.g., insufficient nodes), rollout may hang — consider increasing `maxSurge` or ensuring nodes have capacity.

---

16 — Deliverables & screenshots checklist (lab requirements)

You will be asked to upload screenshots with filenames. Capture and save:

- `Dockerfile.png` — completed Dockerfile (screenshot).
- `crimages.png` — output of `ibmcloud cr images`.
- `app.png` — screenshot of running Guestbook UI.
- `hpa.png` — initial Horizontal Pod Autoscaler output (`kubectl get hpa guestbook`).
- `hpa2.png` — HPA after scaling (replicas increased).
- `upguestbook.png` — pushed updated image v2 output.
- `deployment.png` — output after applying updated deployment (screenshot).
- `up-app.png` — screenshot of updated UI (v2).

- `rev.png` — `kubectl rollout history deployments guestbook --revision=2` output.
- `rs.png` — `kubectl get rs` after rollback showing active ReplicaSet.

How to capture: your lab UI (Skill Network) likely provides a screenshot tool. Otherwise use `scrot` or desktop screenshot and save to the required filename.

---

17 — Appendix

A — Glossary (short, beginner-friendly)

- **Pod** — the smallest deployable unit in Kubernetes; one or more containers that share network & storage.
- **Deployment** — controller that manages ReplicaSets and provides declarative rollouts/rollbacks.
- **ReplicaSet** — ensures a specified number of pod replicas are running; created by Deployments.
- **HPA (Horizontal Pod Autoscaler)** — automatically scales pods based on metrics like CPU. Needs metrics provider.
- **metrics-server** — lightweight aggregator that exposes resource metrics to HPA & `kubectl top`.
- **imagePullPolicy** — controls when Kubelet pulls images (Always, IfNotPresent, Never). Always causes registry checks on pod start.
- **Pod Security Standards (PSS)** — Kubernetes built-in policy levels (privileged / baseline / restricted). Use Pod Security Admission to enforce.

B — Short cheat-sheet of commands (copy-paste)

```
bash
# clone & cd
git clone https://github.com/ibm-developer-skills-network/guestbook
cd guestbook/v1/guestbook

# build & push image
docker build -t us.icr.io/${MY_NAMESPACE}/guestbook:v1 .
ibmcloud cr login
docker push us.icr.io/${MY_NAMESPACE}/guestbook:v1
ibmcloud cr images

# apply k8s
kubectl apply -f deployment.yml
kubectl apply -f service.yml
kubectl autoscale deployment guestbook --cpu-percent=50 --min=1 --max=10

# port-forward
```

```
kubectl port-forward deployment.apps/guestbook 3000:3000

# logging & debug
kubectl get pods -o wide
kubectl logs <pod> -f
kubectl describe hpa guestbook
kubectl rollout history deployment/guestbook
kubectl rollout undo deployment/guestbook --to-revision=1
```

Citations (authoritative sources you can paste into an appendix)

- Kubernetes Horizontal Pod Autoscaler docs.
- Kubernetes Deployments (Rolling update explanation).
- Metrics Server explanation and role for HPA.
- CIS Kubernetes Benchmark (hardening).
- Trivy container image scanning docs & best practice guidance.
- MITRE ATT&CK — Containers matrix & mappings.
- Falco runtime detection & default rules.
- Research on autoscaler/EDoS / Yo-Yo attack vulnerabilities.
- Splunk Kubernetes detection content and logging guidance.
- Port-forward usage documentation.
- Pod Security Standards & Pod Security Admission docs.