# LinuxFoundation.CKS.v2025-05-19.q37

| □□□□: | CKS |
|---|---|
| □□□□: | Certified Kubernetes Security Specialist (CKS) |
| □□□: | Linux Foundation |
| □□ □□ □□□: | 37 |
| □□: | v2025-05-19 |
| # □□ □: | 941 |
| # □□ □□□: | 370 |
| https://www.krdump.com/LinuxFoundation.CKS.v2025-05-19.q37.html | |

**NEW QUESTION: 1**
□□□□□
Trivy□ □□□□ □□ □□□□ □□□□□.
1. □□□ □□□:1
2. k8s.gcr.io/kube-controller-manager:v1.18.6
□□□□ □□□ □□□ □□□□ □□ □□□□ □□ □□ □□□ /opt/trivy-vulnerable.txt□ □□□□□.
**Answer:**
□□ □□ □□□□ □□□□□.

**NEW QUESTION: 2**
□□□ □□ □□ □□□ □□□□ □□□ □□ □□ □□□ □□ □□□□ □□□ □□□ □□□□□ □□□□□.
API □□□□ □□□ □□ □□ □□□ □□ □□□□□. a. RotateKubeletServerCertificate □□□ true□ □□□□ □□□ □□□□□.
b. □□ □□ □□□□ PodSecurityPolicy□ □□□□ □□□ □□□□□.
c. --kubelet-certificate-authority □□□ □□□□ □□□□□□ □□□□□.
Kubelet□ □□ □□□ □□ □□ □□□ □□ □□□□□. a. --anonymous-auth □□□ false□ □□□□ □□□ □□□□□.
b. --authorization-mode □□□ Webhook□□ □□□□ □□□ □□□□□.
ETCD□ □□ □□□ □□ □□ □□□ □□ □□□□□.
a. --auto-tls □□□ true□ □□□□ □□□□ □□□□□□.
b. --peer-auto-tls □□□ true□ □□□□ □□□□ □□□□□□.
□□: Tool Kube-Bench□ □□□□□
**Answer:**
API □□□□ □□□ □□ □□ □□□ □□ □□□□□. a. RotateKubeletServerCertificate □□□ true□ □□□□ □□□ □□□□□.
api□□: v1
□□: □□
□□□□□:
creationTimestamp: null
□□:

□□ □□: kubelet
□□: □□ □□
□□: kubelet
□□□□□□: kube-system
□□:
□□□□:
□□□□:
- □□:
- □□ □□□□ □□□
+ - --□□ □□□=RotateKubeletServerCertificate=□
□□□: gcr.io/google_containers/kubelet-amd64:v1.6.0
□□□□□ □□□:
□□ □□□: 8
http □□□□:
□□□: 127.0.0.1
□□: /healthz
□□: 6443
□□: HTTPS
□□ □□ □: 15
timeout□: 15
□□: kubelet
□□:
□□:
□□: 250M
□□□□□:
- □□□ □□: /etc/kubernetes/
□□: k8s
□□ □□: □
- mountPath: /etc/ssl/certs
□□: □□□
- mountPath: /etc/pki
□□: pki
□□□ □□□□: true
□□:
- □□□ □□:
□□: /etc/kubernetes
□□: k8s
- □□□ □□:
□□: /etc/ssl/certs
□□: □□□
- □□□ □□:

□□: /etc/pki
□□: pki
b. □□ □□ □□□□ PodSecurityPolicy□ □□□□ □□□ □□□□□.
□□: "/bin/ps -ef | grep $apiserverbin | grep -v grep"
□□□:
□□□ □□:
- □□□: "--enable-admission-plugins"
□□□□:
op: □□
□: "PodSecurityPolicy"
□□: □
□□: |
□□□□ □□□ □□□ □□ Pod □□ □□ □□□ □□□□□.
□□ □□ API □□ Pod □□ □□ $apiserverconf□ □□□□□.
□□□ □□□□ --enable-admission-plugins □□□□□ PodSecurityPolicy□ □□□□ □□□ □□□□□.
--enable-admission-plugins=...,PodSecurityPolicy,...
□□ □□ API □□□ □□ □□□□□.
□□: □
c. --kubelet-certificate-authority □□□ □□□□ □□□□□□ □□□□□.
□□: "/bin/ps -ef | grep $apiserverbin | grep -v grep"
□□□:
□□□ □□:
- □□□: "--kubelet-certificate-authority"
□□: □
□□: |
Kubernetes □□□□ □□□ apiserver□ kubelets □□ TLS □□□ □□□□□. □□ □□ API □□ pod □□ □□□ □□□□□.
□□□ □□□□ $apiserverconf□ □□□□ --kubelet-certificate-authority □□□□□ □□ □□□ □□□ □□ □□□ □□□□□.
--kubelet-□□□□□=<ca-□□□>
□□: □
ETCD□ □□ □□□ □□ □□ □□□ □□ □□□□□.
a. --auto-tls □□□ true□ □□□□ □□□□ □□□□□□.
□□□ □□□□ etcd pod □□ □□ $etcdconf□ □□□□ --auto-tls □□□□□ □□□□□ false□ □□□□□. --auto-tls=false b. --peer-auto-tls □□□ true□ □□ □□ □□□□ □□□□□. □□□ □□□□ etcd pod □□ □□ $etcdconf□ □□□□ --peer-auto-tls □□□□□ □□□□□ false□ □□□□□. --peer-auto-tls=false

**NEW QUESTION: 3**
□□□□□
□□ □□□□□□ default□ backend-sa□□ □□□ □ ServiceAccount□ □□□□. □ □□□ default □□□□□□ □□ □□□ □□□ □ □□ □□□ □□□□.
default □□□□□□□ backend-pod□□ □□□ □ Pod□ □□□□, □□ □□□ sa backend-sa□ Pod□ □□□□ □, Pod□ Pod□ □□□ □ □□□ □□□□□.
Pod□ □□ □□□ □□□□□.

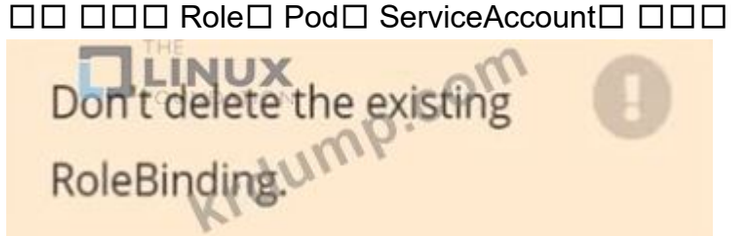
**Answer:**
□□□ □□□ Pod□□ □□□□ □□□□□ □□ ID□ □□□□□.
□□□(□□)□ □□□□□ □□□□□(□: kubectl □□) apiserver□□ □□ □□□ □□(□□□ □□□□ □□□□ □□□□□ □□□ □□□□ □□ □ □□□□□ admin)□□ □□□□□. □□ □□□ □□□□□ □□ □□□□□ apiserver□ □□□ □ □□□□. □□□ □ □ □□ □□□ □□(□: default)□□ □□□□□.
□□□ □□□ □ □□□ □□□ □□□□ □□□ □□□ □□□□□□□ □□ □□□ □□□ □□□□ □□□□□. □□□ □□□ □□ json □□ yaml□ □□□□ (□: kubectl get pods/<podname> -o yaml) spec.serviceAccountName □□□ □□□□ □□□ □□ □ □ □□□□.
□□□□ □□□□□ □□□ □□ □□□□ □□□□ □□□ □□ □□ □□□ □□□□ □□ □□□□ API□ □□□□ □ □□□□. □□□ □□□ API □□□ □□ □□ □□ □□ □□□□□ □□□ □□ □□□□□.
□□ 1.6 □□□□□ □□□ □□□□ automountServiceAccountToken: false□ □□□□ □□□ □□□ □□ API □□ □□ □□ □□□□ □□ □□□ □ □□□□.
api□□: v1
□□: ServiceAccount
□□□□□:
□□: □□ □□
automountServiceAccountToken: □□
...
□□ 1.6 □□□□□ □□ Pod□ □□ API □□ □□ □□ □□□□ □□ □□□ □□ □□□□.
api□□: v1
□□: □□
□□□□□:
□□: my-pod
□□:
serviceAccountName: □□ □□
automountServiceAccountToken: □□
...
□ □ automountServiceAccountToken □□ □□□□ □□ Pod □□□ □□□ □□□□ □□□□□.

**NEW QUESTION: 4**
□□□□□
□□□□□□ □□ □□□ □□□□□□ □□ □□□□ □□□□□ □□□ □□□□□□.
1. □□□ /var/log/kubernetes-logs.txt□ □□□□□.
2. □□ □□□ 12□□ □□□□□.
3. □□ 8□□ □□□ □□ □□ □□□ □□□□□.
4. □□□□ □ □□ □□□ 200MB□ □□□□□
□□ □□□ □□□□ □□□ □□□□□.
1. RequestResponse□□ □□□□□□ □□
2. kube-system □□□□□□□□ □□ □□ □□□ □□ □□□ □□□□□.
3. □□ □□□□ □□ □ □□□ □□ □□ □□□□ □□□□□.
4. □□□□□ □□□□ "pods/portforward", "services/proxy"□ □□□□□.
5. Stage RequestReceived □□
□□□□□ □□□ □□ □□ □□

**Answer:**
□□□□□ □□□ □□□□□ □□ □□ □□ □□□ □□ □□□ □□□□□. Kube-apiserver□ □□□ □□□□□. □□□ □ □□□□ □ □□□ □□□□ □□□ □, □□ □□ □□□ □□ □□ □□□□ □□□□ □□□□□. □□□ □□□ □□□□□ □□□□ □□□□ □□□ □□□□□.
CIS(Center for Internet Security) Kubernetes □□□□ □□□ □□□□ □□□□ □□ □□□ □□□□ □□ □□□□.
□□ cluster.yml □□□ □□□□ □□□□□ □□ □□□ □□□□ □ □□□□.
□□□:
□□ API:
□□ □□:
□□□□: true
□□ □□□ □□□□□ /etc/kubernetes/audit-policy.yaml□□ □□□□ □ □ □□□ □□□. □□ □□□□ JSONlines □□□ □□□ □□ □□□□ □□□□□. □ □ kube-apiserver □□□□ □□□□ □□ □□ □□□□ □□□ □ □□□□.
--audit-log-path□ □□ □□□□ □□ □□□□ □□□□ □ □□□□ □□ □□ □□□ □□□□□. □ □□□□ □□□□ □□□ □□ □□□□ □□□□□□□. - □ □ □□□ □□□□□.
--audit-log-maxage□ □□□ □□ □□ □□□ □□□ □□ □□□ □□□□□□.
--audit-log-maxbackup□ □□□ □□ □□ □□□ □□ □□ □□□□□.
--audit-log-maxsize□ □□□□□□ □□ □□ □□ □□□ □□ □□□ □□□□□ □□□ □□□□□. □□□□□ □□ □□□ kube-apiserver□ Pod□ □□□□ □ □ □□ □□□ □□ □□□ □□□ hostPath□ □□□□□ □□ □□□□ □□□□□ □□ □□□. □□ □□:
--□□ □□ □□=/etc/kubernetes/□□ □□.yaml \
--□□ □□ □□=/var/log/audit.log

**NEW QUESTION: 5**
□□□□□□ test-system□□ □□ □□ test-web-pod□□ □□ Pod□ □□ □□ sa-backend□□ □□□ Pod □□□ □□□ □□□□ □□ □□□ □□□□ □□□ □□□□ get □□□ □□□□□ □□□□□.
statefulset □□□ □□□□ □□ □□□ □□□ □ □□ test-system □□□□□□□ test-system-role-2□□ □ □□□ □□□□.
**Answer:**
test-system-role-2-binding□□□ □□□ □ RoleBinding□ □□□□ □□ □□□ Role□ Pod□ ServiceAccount sa-backend□ □□□□□□.

**NEW QUESTION: 6**
□□
Pod□ ServiceAccount□ □□□□ □□□ □□□□ □□□ □□□ □□□□□. □□ □□□ □□□□ □□ □□□ □□□□□.
□
□□□□□□ security□□ □□ □□ web-pod□□ □□ Pod□ □□□ □□.
Pod□ ServiceAccount sa-dev-1□ □□□□ □□ □□□ □□□□ □□□ □□□ □□□□ □□□□ □□ □□□ □□□□□ □□□□□.
□□□□□□ security□ role-2□□ □ □□□ □□□□. □ □□□ □□□□□□ □□□ □□□□ □□□□ □□□□ □□□ □□□□ □□ □□□□□.
□□ □□□ Role□ Pod□ ServiceAccount□ □□□□□ role-2-binding□□□ □□□ □ RoleBinding□ □□□□□.




**Answer:**

```
candidate@cli:~$ kubectl config use-context KSCH00201
Switched to context "KSCH00201".
candidate@cli:~$ kubectl get pods -n security
NAME      READY   STATUS    RESTARTS   AGE
web-pod   1/1     Running   0          6h9m
candidate@cli:~$ kubectl get deployments.apps -n security
No resources found in security namespace.
candidate@cli:~$ kubectl describe rolebindings.rbac.authorization.k8s.io -n security
Name:         dev-role
Labels:       <none>
Annotations:  <none>
Role:
  Kind:  Role
  Name:  dev-role
Subjects:
  Kind           Name    Namespace
  ----           ----    ---------
  ServiceAccount  sa-dev-1
candidate@cli:~$ kubectl describe role dev-role -n security
Name:         dev-role
Labels:       <none>
Annotations:  <none>
PolicyRule:
  Resources  Non-Resource URLs  Resource Names  Verbs
  ---------  -----------------  --------------  -----
  *          []                 []              [*]
candidate@cli:~$ kubectl edit role/dev-role -n security
```

```
  uid: b4c9ddd6-2729-43bd-8fbd-b2d227f4c4cd
rules:
- apiGroups:
  - ""
  resources:
  - services
  verbs:
  - watch
```

```
candidate@cli:~$ kubectl describe role dev-role -n security
Name:         dev-role
Labels:       <none>
Annotations:  <none>
PolicyRule:
  Resources  Non-Resource URLs  Resource Names  Verbs
  ---------  -----------------  --------------  -----
  *          []                 []              [*]
candidate@cli:~$ kubectl edit role/dev-role -n security
role.rbac.authorization.k8s.io/dev-role edited
candidate@cli:~$ kubectl describe role dev-role -n security
Name:         dev-role
Labels:       <none>
Annotations:  <none>
PolicyRule:
  Resources  Non-Resource URLs  Resource Names  Verbs
  ---------  -----------------  --------------  -----
  services   []                 []              [watch]
candidate@cli:~$ kubectl get pods -n security
NAME      READY   STATUS    RESTARTS   AGE
web-pod   1/1     Running   0          6h12m
candidate@cli:~$ kubectl get pods/web-pod -n security -o yaml | grep serviceAccount
  serviceAccount: sa-dev-1
  serviceAccountName: sa-dev-1
      - serviceAccountToken:
candidate@cli:~$ kubectl create role role-2 --verb=update --resource=namespaces -n security
role.rbac.authorization.k8s.io/role-2 created
candidate@cli:~$ kubectl create rolebinding role-2-binding --role
--role   --role=
candidate@cli:~$ kubectl create rolebinding role-2-binding --role=role-2 --serviceaccount=se
curity:sa-dev-1 -n security
rolebinding.rbac.authorization.k8s.io/role-2-binding created
candidate@cli:~$
```



**NEW QUESTION: 7**

□□□□: admission-cluster

□□□ □□: master

□□ □□: worker1

□□ □□□ □□□□ □□□□/□□ □□□□□ □□□ □ □□□□.

[desk@cli] $ kubectl config use-context □□ □□□□

□□:
□□□□ □□□ □□□□ □□□□□ □□□□□□ □□ □□□□ □□□ □□□ □□□□ □□□□□. □□□□ □□□□ □□□ □□□□ □□□ □□□□ □□□ □ □□□ □□□□□.
□:
□□ □□□□ □□□ □□□□ □□□ □□□□□ □□□ □□□□ □□ □□□ □□□□ □□□.
/etc/Kubernetes/config □□□□□ □□□□ □□□ □□ HTTPS □□□□□ https://imagescanner.local:8181/image_policy□ □□ □□□□ □□□□ □□□ □□□ □ □□ □□:
1. □□□ □□□ □□□□ □□ □□□ □□□□□ □□□□□□.
2. □□ □□□ □□□□ □□□ □□□ □□□□□.
3. □□□ HTTPS □□□□□□ □□□□ □□□□□ □□□ □□□□□. □□□□□ □□□ □□□ /home/cert_masters/test-pod.yml□ □□□ □□□ □□□□□ □ □□□□□. □□: □□□□ □□□ □□□□ □□ □□□ /var/log/policy/scanner.log□□ □□ □ □□□□.

**Answer:**

[□□□@cli] $ cd /etc/Kubernetes/config
1. kubeconfig□ □□□□ □□□□□ □□□□□.
[□□□@cli] $ vim kubeconfig.json
"defaultAllow": false # false□ □□
2. ~/.kube/config□□ □□ □□□ □□ □□□□□ □□□□□.
[master@cli] $cat /etc/kubernetes/config/kubeconfig.yaml | grep □□
□□□ □□:
3. ImagePolicyWebhook □□□
[□□□@cli] $ vim /etc/kubernetes/manifests/kube-apiserver.yaml
- --enable-admission-plugins=NodeRestriction,ImagePolicyWebhook # □□□ □□□□□
- --admission-control-config-file=/etc/kubernetes/config/kubeconfig.json # □ □□□ □□□□□
[desk@cli] $ ssh □□□
[□□□@cli] $ cd /etc/Kubernetes/config
[□□□@cli] $ vim kubeconfig.json

```
{
"imagePolicy": {
"kubeConfigFile": "/etc/kubernetes/config/kubeconfig.yaml",
"allowTTL": 50,
"denyTTL": 50,
"retryBackoff": 500,
"defaultAllow": true # □□□ □□□□□
"defaultAllow": false # □□□ □□□□□
}
}
```

```
{
  "imagePolicy": {
    "kubeConfigFile": "/etc/kubernetes/config/kubeconfig.yaml",
    "allowTTL": 50,
    "denyTTL": 50,
    "retryBackoff": 500,
    "defaultAllow": true   # Delete this
    "defaultAllow": false  # Add this
  }
}
```

□□: □□□ □□□ □□ □ □ □□□□ □ □□ □□□ □□ □ □□□□?

[master@cli] $cat ~/.kube/config | grep □□

□□

[□□□@cli] $cat /etc/kubernetes/manifests/kube-apiserver.yaml

```
controlplane $ cat ~/.kube/config | grep server
    server: https://172.17.0.36:6443
```

[□□□@cli] $vim /etc/kubernetes/config/kubeconfig.yaml

```
apiVersion: v1
kind: Config
clusters:
  - cluster:
      certificate-authority: /etc/kubernetes/config/ca.pem
      server: https://172.17.0.36:6443    #Add this
    name: kubernetes
  - cluster:
contexts:
- context:
    cluster: kubernetes
    user: kube-admin
  name: webhook
current-context: webhook
users:
  - name: kube-admin
    user:
      client-certificate: /etc/kubernetes/config/cert.pem
      client-key: /etc/kubernetes/config/key.pem
```

[master@cli] $ vim /etc/kubernetes/manifests/kube-apiserver.yaml - --enable-admission-plugins=NodeRestriction # □□□ □□□□□ - --enable-admission-plugins=NodeRestriction,ImagePolicyWebhook # □□□ □□□□□ - --admission-control-config-file=/etc/kubernetes/config/kubeconfig.json # □□□ □□□□□ □□: https://kubernetes.io/docs/reference/access-authn-authz/admission-controllers/

- --enable-admission-plugins=NodeRestriction # □□□ □□□□□
- --enable-admission-plugins=NodeRestriction,ImagePolicyWebhook # □□□ □□□□□
- --admission-control-config-file=/etc/kubernetes/config/kubeconfig.json # □□□ □□□□□
[master@cli] $ vim /etc/kubernetes/manifests/kube-apiserver.yaml - --enable-admission-plugins=NodeRestriction # □□□ □□□□□ - --enable-admission-plugins=NodeRestriction,ImagePolicyWebhook # □□□ □□□□□ - --admission-control-config-file=/etc/kubernetes/config/kubeconfig.json # □□□ □□□□□ □ □: https://kubernetes.io/docs/reference/access-authn-authz/admission-controllers/

**NEW QUESTION: 8**
□□□□: □□□□: gvisor □□□ □□: master1 □□□ □□: worker1
□□ □□□ □□□□ □□□□/□□ □□□□□ □□□ □ □□□□.
[desk@cli] $ kubectl config use-context gvisor
□□□□: □ □□□□□ □□ □□□□□□ □□□ □□□ □□□, runsc□ □□□□□ □□□□□□□.
□□: □□□ □□□ □□□ □□ runsc□ □□□□ not-trusted□□ □□□ RuntimeClass□ □□□□. □□□□□□ server□ □□ Pod□ □□□□□□ newruntime□ □ □□□□□.
**Answer:**

**1. Create runtime class by the name of not-trusted using runsc handler**

```
apiVersion: node.k8s.io/v1
kind: RuntimeClass
metadata:
  name: not-trusted
handler: runsc
```

**2. Find all the pods/deployment and edit runtimeClassName parameter to not-trusted under spec**

**[desk@cli] $** `k edit deploy nginx`

```
spec:
  runtimeClassName: not-trusted. # Add this
```

□□
[desk@cli] $vim □□□.yaml
api □□: node.k8s.io/v1
□□: RuntimeClass
□□□□□:
□□: □□□ □ □□
□□□: runsc
[desk@cli] $ k □□ -f □□□.yaml [desk@cli] $ k □□ □□□□
□□ □□ □□ □□□ □□
nginx-6798fc88e8-chp6r 1/1 □□ 0 11m
nginx-6798fc88e8-fs53n 1/1 □□ 0 11m
nginx-6798fc88e8-ndved 1/1 □□ 0 11m
[desk@cli] $ k □□□□
□□ □□□ □□ □□ □□
nginx 3/3 11 3 5m
[desk@cli] $ k □□ nginx □□

```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  labels:
    app: nginx
  name: nginx
spec:
  replicas: 3
  selector:
    matchLabels:
      app: nginx
  strategy: {}
  template:
    metadata:
      labels:
        app: nginx
    spec:
      runtimeClassName: not-trusted     # Add this
      containers:
      - image: nginx
        name: nginx
        resources: {}
status: {}
```



**NEW QUESTION: 9**
runsc□□ □□□ □□□ □□□□ □□□□ untrusted□□ □□□ RuntimeClass□ □□□□.
gVisor □□□ □□□□□ □□□□□ default □□□□□□□ alpine:3.13.2 □□□□ Pod□ □□□□.
**Answer:**

□□: □□□ □□□□ dmesg□ □□□□ □□□ □□ □□□ □□□□□.


**NEW QUESTION: 10**

□□□□□

□□□□□□ testing□ □□ □□□ □□ □ □□ □□□□ □□□□ deny-all□□□ □ NetworkPolicy□ □□□□.

**Answer:**

□□ Pod□ □□□□□ □□ Pod□ □□ □□ □□□□ □□□□ □□ NetworkPolicy□ □□□□ □□□□□□□ □□ "□□" □□ □□□ □□□ □ □□□□.

---

api □□: networking.k8s.io/v1

□□: NetworkPolicy

□□□□□:

□□: default-deny-ingress

□□:

□□ □□□: {}

□□ □□: □□ □□□ □□□ □ □□□□.

---

api □□: networking.k8s.io/v1

□□: NetworkPolicy

□□□□□:

□□: □□ □□ □□

□□:

□□ □□□: {}

□□:

- {}

□□ □□:

- □□

□□□□□ □□ □□ □ □□ □□□□ □□□□□.

□□□□□□□ □□ NetworkPolicy□ □□□□ □□ □□ □ □□ □□□□ □□□□ □□□□□□□ □□ "□□" □□□ □□□ □ □□□□.

---

api □□: networking.k8s.io/v1

□□: NetworkPolicy

□□□□□:

□□: default-deny-all
□□:
□□ □□□: {}
□□ □□:
- □□
- □□
□□□ □□ □□ NetworkPolicy□ □□ □□□□ □□ Pod□□□ □□ □□ □□ □□□□ □□□□ □□□□.

**NEW QUESTION: 11**
□□□□□□ test-system□□ □□ □□ nginx-pod□□ □□ Pod□ □□ □□, □□□ □□□ □□ □□□ □□□□ □□□ /candidate/KSC00124.txt□ □□□□. □ □□□□□ test-system□ □□□□□□ □□□ □□□□ □□ □□□□ □□□ □□□ □ □□ dev-test-role□□□ □ □□□ □□□□.
**Answer:**
dev-test-role-binding□□□ □□□ □□□ RoleBinding□ □□□□□. □□ □□ □□□ Role□ Pod□ ServiceAccount(□□□□□□ test-system□□ □□□□ Nginx Pod□□ □□ □ □□)□ □□□□□□.

**NEW QUESTION: 12**
□□□□ □□□ □□□ □□ 389□□ □□□□ □□□, □□□□□ □□□□ ID□ □□, /candidate/KH77539/files.txt □□□ □□ □□ □□ □□□ □□□ □□□□, □□□□□ □□□□□.
**Answer:**
□□# netstat -ltnup
□□ □□□ □□(□□□)
Proto Recv-Q Send-Q □□ □□ □□ □□ □□ PID/□□□□ □□ tcp 0 0 127.0.0.1:17600 0.0.0.0:* LISTEN 1293/dropbox tcp 0 0 127.0.0.1:17603 0.0.0.0:* LISTEN 1293/dropbox tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN 575/sshd tcp 0 0 127.0.0.1:9393 0.0.0.0:* LISTEN 900/perl tcp 0 0 :::80 :::* LISTEN 9583/docker-proxy tcp 0 0 :::443 :::* LISTEN 9571/□□ □□□ UDP 0 0 0.0.0.0:68 0.0.0.0:* 8822/dhcpcd
...
□□# netstat -ltnup | □□□ ':22'
tcp 0 0 0.0.0.0:22 0.0.0.0:* □□ 575/sshd
ss □□□ netstat □□□ □□□□□.
□□ ss □□□ □□□□ □□ 22□□ □□ □□□□□ □□ □□□ □□□□ □□□ □□□□□□□.
□□# ss -ltnup '□□□ = :22'
Netid □□ Recv-Q Send-Q □□ □□:□□ □□ □□:□□
tcp LISTEN 0 128 0.0.0.0:22 0.0.0.0:* □□□:("sshd",pid=575,fd=3))

**NEW QUESTION: 13**
a. □□□ □□□□□□□ □□ default-token-xxxxx□□ □□ □□□ □□□ □□□□□.
□□□ □□ token.txt□ □□□□□
b. □□ □□□□ DB □□□□□□□ test-db-secret□□□ □ □□□ □□□□.
□□□ □□: mysql
□□□□: password@123
□□ /etc/mysql-credentials□ □□□ □□ test-db-secret□ □□□□ □ □□ □□□□□□ db□ □□□ nginx□ Pod □□ test-db-pod□ □□□□□.

**Answer:**
□□□□, □□ □□ □□□□□ Kubernetes □□□□□ □□□□□ □□□ □□□□□.
□□□□ □□□□□:
□□□□ □□ □□□□□ □□ □□□□ □□ > Kubernetes □□□□□□.
□□ □□ □□□□□ □□ □□□ Kubernetes □□□□□□.
□□□□ □□ □□□□□ □□ □□□ □□ > Kubernetes □□□□□□.
Kubernetes □□□□ □□□ □□□□□.
□□ □□□□ □□ □□ □□□□ □□ □□□ □□□□□.
Kubernetes □□□□ □□(□□) - □□□□□ □□□□□ □□□□□.
□□ □□(□□) - □ □□□□□ □□□ □□□□□.
API URL(□□) - GitLab□ Kubernetes API□ □□□□□ □ □□□□ URL□□□. Kubernetes□ □□ API□ □□□□, □□□ □□ API□ □□□ "□□" URL□ □□ □□. □□ □□, https://kubernetes.example.com/api/v1□ □□ https://kubernetes.example.com□□□.
□□ □□□ □□□□ API URL□ □□□□.
kubectl cluster-info | grep -E 'Kubernetes master|Kubernetes control plane' | awk '/http/ {print $NF}' CA □□□(□□) - □□□□□ □□□□□ □□□ Kubernetes □□ □□ □□□□□. □□□□□ □□□ □□□□ □□□□□.
kubectl get secrets□ □□□ □□□□, □□□ default-token-xxxxx□ □□□ □□□ □□□ □□□. □□□□ □□□ □□ □□□ □□□□□.
□□ □□□ □□□□ □□□□ □□□□.
kubectl get secret <□□ □□> -o jsonpath="{['data']['ca\.crt']}"

**NEW QUESTION: 14**
□□ □□□□□□ default□ backend-sa□□ □□□ □ ServiceAccount□ □□□□. □ □□□ default □□□□□□ □□ □□□ □□□ □ □□ □□□ □□□□.
default □□□□□□□ backend-pod□□ □□□ □ Pod□ □□□□, □□ □□□ sa backend-sa□ Pod□ □□□□ □, Pod□ Pod□ □□□ □ □□□ □□□□□.
Pod□ □□ □□□ □□□□□.
**Answer:**
□□□ □□□ Pod□□ □□□□ □□□□□ □□ ID□ □□□□□.
□□□(□□)□ □□□□□ □□□□□(□: kubectl □□) apiserver□□ □□ □□□ □□(□□□ □□□□ □□□□ □□□□□ □□□ □□□□ □□ □ □□□□□ admin)□□ □□□□□. □□ □□□ □□□□□ □□ □□□□□ apiserver□ □□□ □ □□□□. □□□ □ □ □□ □□□ □□(□: default)□□ □□□□□.
□□□ □□□ □ □□□ □□□ □□□□ □□□ □□□ □□□□□□□ □□ □□□ □□□ □□□□ □□□□□. □□□ □□□ □□ json □□ yaml□ □□□□ (□: kubectl get pods/<podname> -o yaml) spec.serviceAccountName □□□ □□□□ □□□ □□ □ □ □□□□.
□□□□ □□□□□ □□□ □□ □□□□ □□□□ □□□ □□ □□ □□□ □□□□ □□ □□□□ API□ □□□□ □ □□□□. □□□ □□□ API □□□ □□ □□ □□ □□ □□□□□ □□□ □□ □□□□□.
□□ 1.6 □□□□□ □□□ □□□□ automountServiceAccountToken: false□ □□□□ □□□ □□□ □□ API □□ □□ □□ □□□□ □□ □□□ □ □□□□.
api□□: v1
□□: ServiceAccount
□□□□□:
□□: □□ □□
automountServiceAccountToken: □□
...
□□ 1.6 □□□□□ □□ Pod□ □□ API □□ □□ □□ □□□□ □□ □□□ □□ □□□□.
api□□: v1

□□: □□
□□□□□:
□□: my-pod
□□:
serviceAccountName: □□ □□
automountServiceAccountToken: □□
...
□ □ automountServiceAccountToken □□ □□□□ □□ Pod □□□ □□□ □□□□ □□□□□.

**NEW QUESTION: 15**
□□□□□
□□□□□ □□□□ □□□ □□□□ □□□□□.
□□□□□ □□□□ □□□ □□□ □□
/etc/kubernetes/confcontrol □ HTTPS □□□□□ https://test-server.local.8081/image_policy□ □□ □□□ □□□□ □□□ □□□
1. □□ □□□□□ □□□□□□.
2. □□ □□□ □□□□ □□□ □□□ □□□□□.
□□□□□, □□□ □□□ □□□ Pod□ □□□□ □□□ □□□□□□.
**Answer:**
□□ □□ □□□□ □□□□□.

**NEW QUESTION: 16**
□□□□: □□□□: prod □□□ □□: master1 □□□ □□: worker1
□□ □□□ □□□□ □□□□/□□ □□□□□ □□□ □ □□□□.
[desk@cli] $ kubectl config use-context prod
□□: □□□ Dockerfile(ubuntu:18:04 □□□ □□) /home/cert_masters/Dockerfile□ □□□□ □□□□ □□□ □□□□ □ □□ □□(□□□ □□/□□ □□ □□)□ □□□□□.
□□□ □□□□□ □□ /home/cert_masters/mydeployment.yaml□ □□□□ □□□□ □□□ □□□□ □ □□(□□/□□ □□ □□)□ □□□□□.
□□: □□ □□□ □□□□□ □□□□ □□□□. □□ □□ □□□ □□□□ □ □□ □□□ □ □□ □□/□□ □□ □□□ □□ □□□ □□□□. □□□ □□□ □ □ □□□□ □□□ □□ □□□ ID□ 65535□ nobody □□□□ □□□□□□.
**Answer:**
1. Dockerfile□ □□: Dockerfile□ □□□ □□ □ □□□ □□ □□ 2. mydeployment.yaml□ □□: □□ □□□□ □□ □□
[desk@cli] $ vim /home/cert_masters/Dockerfile
ubuntu:latest□□ # □□□ □□□□□
ubuntu:18.04□□ # □□□ □□□□□
USER root # □□□ □□□□□
USER nobody # □□□ □□□□□
apt get install -y lsof=4.72 wget=1.17.1 nginx=4.2□ □□□□□.
ENV □□=□□□
USER root # □□□ □□□□□
USER nobody # □□□ □□□□□

CMD ["nginx -d"]

```
FROM ubuntu:latest   # Remove this
FROM ubuntu:18.04    # Add this
USER root            # Remove this
USER nobody          # Add this
RUN apt get install -y lsof=4.72 wget=1.17.1 nginx=4.2
ENV  ENVIRONMENT=testing
USER root            # Remove this
USER nobody          # Add this
CMD ["nginx -d"]
```



[desk@cli] $ vim /home/cert_masters/mydeployment.yaml

api□□: apps/v1

□□: □□

□□□□□:

creationTimestamp: null

□□:

□: □□□

□□: □□□

□□:

□□□: 1

□□□:

□□□□:

□: □□□

□□: {}

□□:

□□□□□:

creationTimestamp: null

□□:

□: □□□

□□:

□□□□:

- □□□: bitnami/kafka

□□: □□□

□□□□□:

- □□: □□□-vol

□□□ □□: /var/lib/kafka

□□ □□□□:

{"capabilities":{"add":["NET_ADMIN"],"drop":["all"]},"privileged": True,"readOnlyRootFilesystem": False, "runAsUser": 65535} # □□□ □□□□□.
{"capabilities":{"add":["NET_ADMIN"],"drop":["all"]},"privileged": False,"readOnlyRootFilesystem": True, "runAsUser": 65535} # □ □□□□ □□□□□: {} □□:
- □□: □□□-vol
emptyDir: {}
□□: {}
□□ □□: [desk@cli] $ vim /home/cert_masters/mydeployment.yaml

```
apiVersion: apps/v1
kind: Deployment
metadata:
  creationTimestamp: null
  labels:
    app: kafka
  name: kafka
spec:
  replicas: 1
  selector:
    matchLabels:
      app: kafka
  strategy: {}
  template:
    metadata:
      creationTimestamp: null
      labels:
        app: kafka
    spec:
      containers:
      - image: bitnami/kafka
        name: kafka
        volumeMounts:
          - name: kafka-vol
            mountPath: /var/lib/kafka
        securityContext:
          {"capabilities":{"add":["NET_ADMIN"],"drop":["all"]},"privileged": True,"readOnlyRootFilesystem": False, "runAsUser": 65535} # Delete This
          {"capabilities":{"add":["NET_ADMIN"],"drop":["all"]},"privileged": False,"readOnlyRootFilesystem": True, "runAsUser": 65535} # Add This
        resources: {}
      volumes:
      - name: kafka-vol
        emptyDir: {}
status: {}
```





**NEW QUESTION: 17**
□□ □□□ □□□□ □□□□/□□ □□□□□ □□□ □ □□□□. [desk@cli] $ kubectl config use-context test-account □□: □□□□□□ □□ □□□ □□□□ □□.
□□□ □□□ □□ □□□□ □□□□□ □□ □□□ □□□□□.
1. □□□ /var/log/Kubernetes/logs.txt□ □□□□□.
2. □□ □□□ 5□□ □□□□□.
3. □□ 10□□ □□□ □□ □□ □□□ □□□□□.
□□ □□□ /etc/Kubernetes/logpolicy/audit-policy.yaml□ □□□□□. □□□□ □□ □□□ □□□□□. □□: □□ □□□ □□□□□ □□□ □□□ □□□□.
□□ □□□ □□□□ □□□□ □□□ □□□□□. 1. RequestResponse □□□□ □□ □□ 2. □□□□□□ □□□□□□□ persistentvolumes□ □□ □□ □□ 3. □□□□□ □□□□ □□ □□□□□□□ ConfigMap □ Secret □□ □□ □□□□□ □□□□ □□ □□ □□□ □□□□ □□□□ □□□ □□□□□. □□: □□ □ □□□ □□□□ □□ □□ □□□.

**Answer:**

$ vim /etc/kubernetes/log-policy/audit-policy.yaml

- □□: □□□□

□□□ □□: ["□□□:□□"]

- □□: □□

□□:

- □□: "" # □□ API □□

□□□: ["persistentvolumes"]

□□□□□□: ["□□□□□"]

- □□: □□□□□

□□:

- □□: ""

□□□: ["configmaps", "secrets"]

- □□: □□□□□

$ vim /etc/kubernetes/manifests/kube-apiserver.yaml □□□ □□□□□.

- --□□ □□ □□=/etc/kubernetes/log-policy/audit-policy.yaml

- --□□ □□ □□=/var/log/kubernetes/logs.txt

- --□□+□□+□□□=5

- --□□+□□+□□□□=10

□□

[desk@cli] $ ssh master1 [master1@cli] $ vim /etc/kubernetes/log-policy/audit-policy.yaml apiVersion: audit.k8s.io/v1 # □□□□□.

□□: □□

# RequestReceived □□□□ □□ □□□ □□ □□ □□□□ □□□□ □□□.

□□□□:

- "□□ □□□"

□□:

# □□□□□ □□ □□□□□ "system:kube-proxy"□ □□ □□ □□□ □□□□ □□□□.

- □□ : □□

□□□: ["system:kube-proxy"]

□□: ["watch"]

□□:

- □□: "" # □□ API □□

□□□: ["□□□□□", "□□□"]

# □□ □□□□ URL □□□ □□ □□□ □□□ □□□□ □□□.

- □□ : □□

□□□ □□: ["□□□:□□□"]

□□□URLs:

- "/api*" # □□□□□ □□.

- "/□□"

# □□□ □□ □□□ □□□□□

- □□: □□□□
userGroups: ["system:nodes"] # □□ □□
- □□: □□
□□:
- □□: "" # □□ API □□
□□□: ["persistentvolumes"] # persistentvolumes□ □□ □□
□□□□□□: ["frontend"] # frontend ns□ □□ □□□ □□□□□.
- □□: □□□□□
□□:
- □□: "" # □□ API □□
□□□: ["configmaps", "secrets"] # configmaps □ secrets □□
- □□: □□□□□ # □ □ □□ □□ □□ □□
[master1@cli] $ vim /etc/kubernetes/manifests/kube-apiserver.yaml
api□□: v1
□□: □□
□□□□□:
□□:
kubeadm.kubernetes.io/kube-apiserver.advertise-address.endpoint: 10.0.0.5:6443 □□□:
□□ □□: kube-apiserver
□□: □□ □□
□□: kube-apiserver
□□□□□□: kube-system
□□:
□□□□:
- □□:
- be-apiserver
- --□□ □□=10.0.0.5
- --□□+□□=□
- --authorization-mode=□□, RBAC
- --audit-policy-file=/etc/kubernetes/log-policy/audit-policy.yaml # □□□ □□□□□
- --audit-log-path=/var/log/kubernetes/logs.txt # □□□ □□□□□
- --audit-log-maxage=5 # □□□ □□□□□
- --audit-log-maxbackup=10 # □□□ □□□□□
...
□□□ □□□□□
□□: □□ □□ □ □□ □□□ □□ vim /etc/kubernetes/manifests/kube-apiserver.yaml□ □□□□□ □□□□ □□□□ □□□ □□□□. □□:
https://kubernetes.io/docs/tasks/debug-application-cluster/audit/

**NEW QUESTION: 18**

□□ □□□□/□□□□ □ □□□ □□□□ □□□.□□□□: immutable-cluster □□□ □□: master1 □□□ □□: worker1 □□ □□□ □□□□ □□□□/□□ □ □□□□ □□□ □ □□□□.[desk@cli] $ kubectl config use-context immutable-cluster □□□□: □□□□□ □□ □□□ □ □□□□ □□□□ □□ □□ □□□□. □□: prod □□□□□□□□ □□ □□ Pod□ □□□□ □□ □□□□ □□□□ □□□ □□ □□ Pod□ □□□□□.□□ □□□ □ □□□ □□ □□□ □□ □□□ □□□ □□□□□.1. □□□□ □□□ □□□□ □□□ □ □□ Pod□ □□ □□□□ □□ □□□ □□□□ □□□.□□: □□□□ □□□ □□□□ □□□ □□□□ □□□ □□□ □□ □□□ □□□ □□□□.2. □□ □□□□ □□□ □□□ □□□ Pod□ □□□□□ □□ □□□□ □□□□ □□□ □□ □□□ □□□□ □□□.

**Answer:**

```
candidate@cli:~$ kubectl config use-context KSRS00501
Switched to context "KSRS00501".
candidate@cli:~$ kubectl get pod -n testing
NAME       READY   STATUS    RESTARTS   AGE
app        1/1     Running   0          6h31m
frontend   1/1     Running   0          6h32m
smtp       1/1     Running   0          6h31m
candidate@cli:~$ kubectl get pod/app -n testing -o yaml
    - lastProbeTime: null
      lastTransitionTime: "2022-05-20T08:40:35Z"
      status: "True"
      type: PodScheduled
    containerStatuses:
    - containerID: docker://11143682c400984c9faf3dff1e056d4b00a7eb1de007fe1834be0a84fa146e18
      image: nginx:latest
      imageID: docker-pullable://nginx@sha256:2d17cc4981bf1e22a87ef3b3dd20fbb72c3868738e3f3076
62eb40e2630d4320
      lastState: {}
      name: app-container
      ready: true
      restartCount: 0
      started: true
      state:
        running:
          startedAt: "2022-05-20T08:40:37Z"
    hostIP: 10.240.86.141
    phase: Running
    podIP: 10.10.1.3
    podIPs:
    - ip: 10.10.1.3
    qosClass: BestEffort
    startTime: "2022-05-20T08:40:35Z"
candidate@cli:~$ kubectl get pod/app -n testing -o yaml | grep -E 'privileged|ReadOnlyFileSy
stem'
      privileged: true
candidate@cli:~$ kubectl get pod/frontend -n testing -o yaml | grep -E 'privileged|ReadOnlyF
ileSystem'
      privileged: false
```

```
candidate@cli:~$ kubectl get pod/smtp -n testing -o yaml | grep -E 'privileged|ReadOnlyFileS
ystem'
      privileged: true
candidate@cli:~$ kubectl get pod -n testing -o yaml | grep -i ReadOnly
        readOnlyRootFilesystem: false
        readOnly: true
        readOnlyRootFilesystem: true
        readOnly: true
        readOnlyRootFilesystem: false
        readOnly: true
candidate@cli:~$ kubectl get pod/smtp -n testing -o yaml | grep -E 'privileged|readOnlyRootF
ileSystem'
      privileged: true
candidate@cli:~$ kubectl get pod/app -n testing -o yaml | grep -E 'privileged|readOnlyRootFi
leSystem'
      privileged: true
candidate@cli:~$ kubectl get pod/frontend -n testing -o yaml | grep -E 'privileged|readOnlyR
ootFileSystem'
      privileged: false
candidate@cli:~$ kubectl get pod/frontend -n testing -o yaml | grep -E 'privileged|readOnlyR
ootFilesystem'
      privileged: true
      readOnlyRootFilesystem: false
candidate@cli:~$ kubectl delete pod/app -n testing
pod "app" deleted
candidate@cli:~$ kubectl get pod/smtp -n testing -o yaml | grep -E 'privileged|readOnlyRootF
ilesystem'
      privileged: true
      readOnlyRootFilesystem: false
candidate@cli:~$ kubectl delete pod/smtp -n testing
pod "smtp" deleted
```

□□: https://kubernetes.io/docs/concepts/policy/pod-security-policy/ https://cloud.google.com/architecture/best-practices-for-operating-containers

**NEW QUESTION: 19**

□□□□: qa-cluster

□□□ □□: master □□ □□: worker1

□□ □□□ □□□□ □□□□/□□ □□□□□ □□□ □ □□□□.

[desk@cli] $ kubectl config use-context qa-cluster

□:

dev □□□□□□□□ □□□□ Pod □□□ □□ □□□□ □□□□ □□ restricted-policy□□ □□□ NetworkPolicy□ □□□□□.

□□ Pod□ Pod products-service□ □□□□□ □□□□□.

1. qa □□□□□□□ Pod

2. □□□ environment: stage□ □□ Pod, □□ □□□□□□

**Answer:**

$ k get ns qa --show-labels

□□ □□ □□ □□

qa □□ 47m env=stage
$ k □□ □□□□ -n dev --show-labels
□□ □□ □□ □□□ □□ □□
□□ 1/1 □□ 0 3s env=dev-team
api □□: networking.k8s.io/v1
□□: NetworkPolicy
□□□□□:
□□: □□ □□
□□□□□□: dev
□□:
□□ □□□:
□□□□:
env: dev-team
□□ □□:
- □□
□□:
- □□:
- □□□□□□ □□□:
□□□□:
env: □□
- □□ □□□:
□□□□:
env: □□
[desk@cli] $ k get ns qa --show-labels
□□ □□ □□ □□
qa □□ 47m env=stage
[desk@cli] $ k □□ □□□□ -n dev −−□=□
□□ □□ □□ □□□ □□ □□
□□ 1/1 □□ 0 3s env=dev-team
[desk@cli] $ vim netpol2.yaml
api □□: networking.k8s.io/v1
□□: NetworkPolicy
□□□□□:
□□: □□ □□
□□□□□□: dev
□□:
□□ □□□:
□□□□:
env: dev-team
□□ □□:

- □□
□□:
- □□:
- □□□□□□ □□□:
□□□□:
env: □□
- □□ □□□:
□□□□:
env: □□
[desk@cli] $ k apply -f netpol2.yaml □□: https://kubernetes.io/docs/concepts/services-networking/network-policies/
[desk@cli] $ k apply -f netpol2.yaml □□: https://kubernetes.io/docs/concepts/services-networking/network-policies/

**NEW QUESTION: 20**
□□□□□
□□□ □□ □□□ Falco□ □□□□ Nginx□ □□ □□□□□□ □□ □□□□ □□□□ □□□□□ □□□□ □□□ □□□□ □□ 20□ □□ □□□□ □□□ □ □□□□.
□□□ □□□ □□□□ □□ □□ art /opt/falco-incident.txt□ □□□□□. □ □□ □□□, □□:
[□□□□□],[uid],[□□□□ □□]
**Answer:**
□□ □□ □□□□ □□□□□.

**NEW QUESTION: 21**
□□□□□
□□□ □□ □□ Falco□ □□□□ □□ □□□□ □□ □□ □□□□□ □□□□ □□□ □□□□ □□ 30□ □□ □□□□ □□□ □□□□ □□□ □□□□□ □ □□□ □□□□ □□ art /opt/falco-incident.txt□ □□□□□. □□□ □□ □□□□□□.
[□□□□□],[uid],[□□□ □□],[□□□□ □□]
**Answer:**
□□□ □□□ □□□□□

**NEW QUESTION: 22**
john□□□ □□□□ □□□, CSR □□□ □□□, □□ □ □□□□ □□□□ □□□□□.
□□□□□□ john□ □□□ □□□ □□□□□ john-role□□□ □□ □□□ □□□□.
□□□□□ john-role-binding□□□ RoleBinding□ □□□□ □□ □□□ □□ john-role□ □□□□□□ john□ □□ □□□ john□ □□□□□.
□□ □□: kubectl auth CLI □□□ □□□□ □□□ □□□□□.
**Answer:**
se kubectl□ □□□□ CSR□ □□□ □□□□□.
CSR □□□ □□□□:
kubectl csr □□
CSR □□:
kubectl □□□ □□ myuser
□□□□ □□□□

CSR□□ □□□□ □□□□□.
kubectl get csr/myuser -o yaml
□□□ John□□ NEW_CRD □□□□ □□□ □ □□ □□□ □□□□ □□□ □□ □□□□□□.
kubectl □□ -f roleBindingJohn.yaml --as=john
rolebinding.rbac.authorization.k8s.io/john_external-rosource-rb □□ □□: RoleBinding apiVersion: rbac.authorization.k8s.io/v1 □□□□□:
□□: john_crd
□□□□□□: development-john
□□:
- □□ : □□□
□□: □
api□□: rbac.authorization.k8s.io
roleRef:
□□: ClusterRole
□□: crd-creation
□□: ClusterRole
api □□: rbac.authorization.k8s.io/v1
□□□□□:
□□: crd-creation
□□:
- api□□: ["kubernetes-client.io/v1"]
□□□: ["NEW_CRD"]
□□: ["□□□□, □□□□, □□"]

**NEW QUESTION: 23**
□□ □□□□/□□□□ □ □□□ □□□□ □□□.□□□□: trace □□□ □□: master □□□ □□: worker1 □□ □□□ □□□□ □□□□/□□ □□□□□ □□ □ □ □□□□.[desk@cli] $ kubectl config use-context trace □□□ □□: Sysdig □□ Falco □□□ □□□ □ □□□□.□□: □□ □□□ □□□□ Pod tomcat□ □ □ □□ □□□□□□ □□□ □□ □□ □□□□ □□□□ □□□□□ □□ □□□ □□□□□.□□□ □ □□ □□□ □ □□□□□.1. falco 2. sysdig □□□ worker1 □□□□ □□ □□□□ □□□□.□□ □□□□ □□□□ □□□□□ □□□□ □□□ □□□□ □□ 40□ □□ □□□□□ □□□ □□□□□.□□ □□□ □ /home/cert_masters/report□ □□□□ □□□ □□□□□.[timestamp],[uid],[processName] □□: □□□□ □□□ □□□□□ □□□ □□□ □□□□ □□□ □□ □ □□□ □□□.

**Answer:**
$vim /etc/falco/falco_rules.local.yaml
- □□: □□□□ □□□□ □□(□□+□□)
desc: open+create□ □□ □□□□□ □□□ □□ □□□ □□□
□□: >
evt.type(open,openat,creat) □
evt.is_open_exec=true □
□□□□ □
runc_writing_exec_fifo□ □□□
runc_writing_var_lib_docker□ □□□

user_known_container_drift_activities□ □□□
□□□.□□□>=0
□□: >
%evt.time,%user.uid,%proc.name # □□□ □□□□□/falco □□□ □□□□□
□□□□: □□
$kill -1 <Falco□ PID>
□□
[desk@cli] $ ssh node01 [node01@cli] $ vim /etc/falco/falco_rules.yaml □□□□ □□□□□ □□□□□□ □□□□ falco_rules.local.yaml□ □□□□□□.
[node01@cli] $ vim /etc/falco/falco_rules.local.yaml
- □□: □□□□ □□□□ □□(□□+□□)
desc: open+create□ □□ □□□□□ □□□ □□ □□□ □□□
□□: >
evt.type(open,openat,creat) □
evt.is_open_exec=true □
□□□□ □
runc_writing_exec_fifo□ □□□
runc_writing_var_lib_docker□ □□□
user_known_container_drift_activities□ □□□
□□□.□□□>=0
□□: >
%evt.time,%user.uid,%proc.name # □□□ □□□□□/falco □□□ □□□□□
□□□□: □□
[node01@cli] $ vim /etc/falco/falco.yaml


**NEW QUESTION: 24**
□□:
□□□□: gvisor
□□□ □□: master1
□□ □□: worker1
□□ □□□ □□□□ □□□□/□□ □□□□□ □□□ □ □□□□.
[desk@cli] $ kubectl config use-context gvisor
□□□□: □ □□□□□ □□ □□□□□□ □□□ □□□ □□□, runsc□ □□□□□ □□□□□□□.
□:
□□□ □□□ □□□ □□ runsc□ □□□□ not-trusted□□ □□□ RuntimeClass□ □□□□.
□□□□□□ server□ □□ □□ Pod□ newruntime□□ □□□□□ □□□□□□□.

**Answer:**

□□ □□/□□□ □□ □□□ □□ □□□ □ □□ runtimeClassName □□□□□ □□□□□.

[desk@cli] $ k □□ nginx □□

□□:

runtimeClassName: □□□ □ □□. # □□□ □□□□□

□□

[desk@cli] $vim □□□.yaml

api □□: node.k8s.io/v1

□□: RuntimeClass

□□□□□:

□□: □□□ □ □□

□□□: runsc

[desk@cli] $ k □□ -f □□□.yaml

[desk@cli] $ k □□ □□□□

□□ □□ □□ □□□ □□

nginx-6798fc88e8-chp6r 1/1 □□ 0 11m

nginx-6798fc88e8-fs53n 1/1 □□ 0 11m

nginx-6798fc88e8-ndved 1/1 □□ 0 11m

[desk@cli] $ k □□□

□□ □□□ □□ □□ □□

nginx 3/3 11 3 5m

[desk@cli] $ k □□ nginx □□

```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  labels:
    app: nginx
  name: nginx
spec:
  replicas: 3
  selector:
    matchLabels:
      app: nginx
  strategy: {}
  template:
    metadata:
      labels:
        app: nginx
    spec:
      runtimeClassName: not-trusted     # Add this
      containers:
      - image: nginx
        name: nginx
        resources: {}
status: {}
```



**NEW QUESTION: 25**
□□□ YAML □□□□□□ Kubesec Docker □□□□ □□□□ □□□□, □□□ □□ □□□ □□□□ □□□□□, 4□□□ □□□□□□.
□□□□□□.yaml
api□□: v1
□□: □□
□□□□□:
□□: kubesec-demo
□□:
□□□□:
- □□: kubesec-demo

□□□: gcr.io/google-samples/node-hello:1.0
□□ □□□□:
readOnlyRootFilesystem: true
□□: docker run -i kubesec/kubesec:512c5e0 scan /dev/stdin < kubesec-test.yaml
**Answer:**
kubesec □□ k8s-deployment.yaml
□□□ <<EOF > kubesec-test.yaml
api□□: v1
□□: □□
□□□□□:
□□: kubesec-demo
□□:
□□□□:
- □□: kubesec-demo
□□□: gcr.io/google-samples/node-hello:1.0
□□ □□□□:
readOnlyRootFilesystem: true
□□
kubesec □□ kubesec-test.yaml
docker run -i kubesec/kubesec:512c5e0 /dev/stdin □□ < kubesec-test.yaml kubesec http 8080 &
[1] 12345
{"severity":"info","timestamp":"2019-05-12T11:58:34.662+0100","caller":"server/server.go:69","message":"□□ 8080□□ HTTP □□ □□"} curl -sSX POST --data-binary @test/asset/score-0-cap-sys-admin.yml http://localhost:8080/scan
[
{
"object": "Pod/security-context-demo.default",
"□□": □,
"message": "-30□□□ □□□□□□",
"□□": -30,
"□□": {
"□□□□": [
{
"□□□": "□□□□[] .securityContext .capabilities .add == SYS_ADMIN",
"reason": "CAP_SYS_ADMIN□ □□ □□□ □□ □□□□□ □□ □□□ □□□."
},
{
"□□□": "□□□□[] .securityContext .runAsNonRoot == true",
"reason": "□□ □□□ □□□□ □□ □□ □□ □□□□ □□□ □□ □□□□ □□□□□ □□□□□."
},
// ...

**NEW QUESTION: 26**
□□□□: dev
□□□ □□: master1
□□ □□: worker1
□□ □□□ □□□□ □□□□/□□ □□□□□ □□□ □ □□□□.
[desk@cli] $ kubectl config use-context dev
□:
□□□ □□□□□□□ □□ adam□□□ □□□ □□ □□□ □□□ □□□□□.
□□□ □□ □□□ /home/cert-masters/username.txt□□ □□□ □□□□, □□□□ □□□ /home/cert-masters/password.txt□□ □□□ □□□□□.
1. □ □□□ □□ □□□□ □□□. □□ □□□□ □□□□.
2. □□ □□□□ □□□ □□□ □□/□□□□ □□□. □□□ □□ □□□ □□ □□□ □□□□.
□□ □□□ □□□□ □□□ □□□□□□□ newsecret□□□ □ □□ □□□ □□□□.
□□□ □□: dbadmin
□□□□: moresecurepas
□□□□□ □□□ □□ □□ newsecret□ □□□□ □ □□ □□□ Pod□ □□□□□.
□□□□□□: safe
□□ □□: mysecret-pod
□□□□ □□: db-container
□□□: redis
□□ □□: secret-vol
□□□ □□: /etc/mysecret
**Answer:**
1. □□□ □□ □□ □□□□ □□□ □□□□□.
k □□□ □□□□ adam -n safe -o yaml
2. --from-literal□ □□□□ □□□ □□□ □□□□.
[desk@cli] $k □□ □□ □□□□ □□ -n safe --from-literal=□□□ □□=dbadmin --from-literal=□□□□=moresecurepass
3. mysecret-pod□ db-container□ □□□□ □□□□□□.
□□

```
controlplane $ k get secret adam -n safe -o yaml
apiVersion: v1
data:
  password: c2VjcmV0cGFzcw==
  username: Y2VydC1tYXN0ZXJz
kind: Secret
metadata:
  creationTimestamp: "2021-06-13T11:56:32Z"
  managedFields:
  - apiVersion: v1
    fieldsType: FieldsV1
    fieldsV1:
      f:data:
        .: {}
        f:password: {}
        f:username: {}
      f:type: {}
    manager: kubectl-create
    operation: Update
    time: "2021-06-13T11:56:32Z"
  name: adam
  namespace: safe
  resourceVersion: "6405"
  selfLink: /api/v1/namespaces/safe/secrets/adam
  uid: da04fa1e-22a5-49d0-95d5-d73e40542033
type: Opaque
```

```
controlplane $ echo "c2VjcmV0cGFzcw==" | base64 -d | tee -a /home/cert-masters/password.txt
secretpasscontrolplane $
```

[desk@cli] $k □□ □□ newsecret □□ -n safe --from-literal=□□□ □□=dbadmin --from-literal=□□=moresecurepass □□/newsecret □□□

[desk@cli] $vim /home/certs_masters/secret-pod.yaml

api□□: v1

□□: □□

□□□□□:

□□: mysecret-pod

□□□□□□: □□□

□□:

□□: mysecret-pod

□□:

□□□□:

- □□: db-container

□□□: redis

□□□□□:

- □□: secret-vol

mountPath: /etc/mysecret

□□ □□: □

□□:

- □□: secret-vol

□□:

secretName: newsecret

[desk@cli] $ k □□ -f /home/certs_masters/secret-pod.yaml

pod/mysecret-pod □□□

[desk@cli] $ k exec -it mysecret-pod -n safe - cat /etc/mysecret/username dbadmin

```
controlplane $ k exec -it mysecret-pod -n safe -- cat /etc/mysecret/username
dbadmincontrolplane $
```

[desk@cli] $ k exec -it mysecret-pod -n safe - cat /etc/mysecret/password moresecurepas

```
controlplane $ k exec -it mysecret-pod -n safe -- cat /etc/mysecret/password
moresecurepasscontrolplane $
```

**NEW QUESTION: 27**

□□□ YAML □□□□□□ Kubesec Docker □□□□ □□□□ □□□□, □□□ □□ □□□ □□□□ □□□□□, 4□□□ □□□□□□.

□□□ㅋ□□.yaml

api□□: v1

□□: □□

□□□□□:

□□: kubesec-demo

□□:

□□□□:

- □□: kubesec-demo
□□□: gcr.io/google-samples/node-hello:1.0
□□ □□□□:
readOnlyRootFilesystem: true
**Answer:**
□□: docker run -i kubesec/kubesec:512c5e0 scan /dev/stdin < kubesec-test.yaml

**NEW QUESTION: 28**
□□□ □□□□□□□□ □□ □□□□ persistentvolumeclaim□ □□□□ PSP□ □□□□.
persistentvolumeclaim □□ □□ □□□ □□□□□ □□ □□□□ prevent-volume-policy□□ □□□ □□□ PodSecurityPolicy□ □□□□□.
□□□ □□□□□□□ psp-sa□□ □□□ □ ServiceAccount□ □□□□.
□□ □□□ Pod □□ □□ prevent-volume-policy□ □□□□ psp-role□□□ □□□ □ ClusterRole□ □□□□□. □□□ ClusterRole psp-role□ □□□ SA psp-sa □ □□□□□ psp-role-binding□□□ □□□ □ ClusterRoleBinding□ □□□□□.
□□:
□□, Pod Maifest□□ □□□ □□□□ □□ □□□ □□□ □□□□□ □□□□□. □□□□ □□□.
POD □□□:
api□□: v1
□□: □□
□□□□□:
□□:
□□:
□□□□:
- □□:
□□:
□□□□□:
- □□:
□□□ □□:
□□:
- □□:
□□:
□□ □□:
**Answer:**
api □□: policy/v1beta1
□□: SubSecurityPolicy
□□□□□:
□□: □□□
□□:
seccomp.security.alpha.kubernetes.io/allowedProfileNames: 'docker/default,runtime/default' apparmor.security.beta.kubernetes.io/allowedProfileNames: 'runtime/default' seccomp.security.alpha.kubernetes.io/defaultProfileName: 'runtime/default' apparmor.security.beta.kubernetes.io/defaultProfileName: 'runtime/default' □□:

□□: □□
# □□□□ □□□□□□□ □□□□ □ □□□□□.
allowPrivilegeEscalation: □□
# □□□ □□□ □□ + □□ □□□ □□□□ □□ □□ □□□□□.
# □□□ □□□ □□ □□□ □□ □□ □□□ □ □□□□.
□□DropCapabilities:
- □□
# □□ □□ □□□ □□□□□.
□□:
- 'configMap'
- '□ □□□□'
- '□□'
- '□□'
- 'downwardAPI'
# □□□□ □□□□ □□□ persistentVolumes□ □□□□ □□□□□ □□□□□.
- '□□ □□ □□□'
□□□ □□□□: false
□□□IPC: □□
□□□PID: □□
□□□□ □□:
# □□□□□ □□ □□ □□ □□□□□ □□□□□.
□□: 'MustRunAsNonRoot'
se□□□:
# □ □□□ □□□ SELinux□ □□ AppArmor□ □□□□□ □□□□□.
□□: 'RunAsAny'
□□ □□:
□□: 'MustRunAs'
□□:
# □□ □□ □□□ □□□□□.
- □□: 1
□□ : 65535
fs□□:
□□: 'MustRunAs'
□□:
# □□ □□ □□□ □□□□□.
- □□: 1
□□ : 65535
readOnlyRootFilesystem: □□

**NEW QUESTION: 29**

□□:
□□□□: prod
□□□ □□: master1
□□ □□: worker1
□□ □□□ □□□□ □□□□/□□ □□□□□ □□□ □ □□□□.
[desk@cli] $ kubectl config use-context prod
□:
□□□ Dockerfile□ □□□□ □□□□□(ubuntu:18:04 □□□ □□)
/home/cert_masters/Dockerfile□ □□□ □□□□ □ □□ □□, □ □□ □□ □□/□□ □□ □□□ □□□□□.
□□□ □□□□□ □□□ □□□□ □□□□□.
/home/cert_masters/mydeployment.yaml □□□ □□□□ □ □□□ □□□□ □□/□□ □□ □□□ □□ □□□ □□□□□□.
□□: □□ □□□ □□□□□ □□□□ □□□. □□ □□ □□□ □□□□ □ □□ □□ □□□ □ □□ □□/□□ □□ □□□ □□ □□□ □□□.
□□□ □□□ □□ □□□□ □□□ □□ □□□ ID 65535□ □□□□ nobody □□□□ □□□□□.
**Answer:**
1. Dockerfile□ □□: Dockerfile□□ □□□ □□ □ □□□ □□ □□
2. mydeployment.yaml□ □□: □□ □□□□ □□
□□
[desk@cli] $ vim /home/cert_masters/Dockerfile
ubuntu:latest□□ # □□□ □□□□□
ubuntu:18.04□□ # □□□ □□□□□
USER root # □□□ □□□□□
USER nobody # □□□ □□□□□
apt get install -y lsof=4.72 wget=1.17.1 nginx=4.2□ □□□□□.
ENV □□=□□□
USER root # □□□ □□□□□
USER nobody # □□□ □□□□□
CMD ["nginx -d"]

```
FROM ubuntu:latest   # Remove this
FROM ubuntu:18.04    # Add this
USER root            # Remove this
USER nobody          # Add this
RUN apt get install -y lsof=4.72 wget=1.17.1 nginx=4.2
ENV  ENVIRONMENT=testing
USER root            # Remove this
USER nobody          # Add this
CMD ["nginx -d"]
```

[desk@cli] $ vim /home/cert_masters/mydeployment.yaml
api□□: apps/v1
□□: □□

□□□□□:
creationTimestamp: null
□□:
□: □□□
□□: □□□
□□:
□□□: 1
□□□:
□□□□:
□: □□□
□□: {}
□□:
□□□□□:
creationTimestamp: null
□□:
□: □□□
□□:
□□□□:
- □□□: bitnami/kafka
□□: □□□
□□□□□:
- □□: □□□-vol
□□□ □□: /var/lib/kafka
□□ □□□□:
{"capabilities":{"add":["NET_ADMIN"],"drop":["all"]},"privileged": True,"readOnlyRootFilesystem": False, "runAsUser": 65535} # □□□ □□□□□.
{"capabilities":{"add":["NET_ADMIN"],"drop":["all"]},"privileged": False,"readOnlyRootFilesystem": True, "runAsUser": 65535} # □ □□□□ □□□□□: {} □□:
- □□: □□□-vol
emptyDir: {}
□□: {}
□□□□ □□:
[desk@cli] $ vim /home/cert_masters/mydeployment.yaml

```
apiVersion: apps/v1
kind: Deployment
metadata:
  creationTimestamp: null
  labels:
    app: kafka
  name: kafka
spec:
  replicas: 1
  selector:
    matchLabels:
      app: kafka
  strategy: {}
  template:
    metadata:
      creationTimestamp: null
      labels:
        app: kafka
    spec:
      containers:
      - image: bitnami/kafka
        name: kafka
        volumeMounts:
          - name: kafka-vol
            mountPath: /var/lib/kafka
        securityContext:
          {"capabilities":{"add":["NET_ADMIN"],"drop":["all"]},"privileged": True,"readOnlyRootFilesystem": False, "runAsUser": 65535} # Delete This
          {"capabilities":{"add":["NET_ADMIN"],"drop":["all"]},"privileged": False,"readOnlyRootFilesystem": True, "runAsUser": 65535} # Add This
        resources: {}
      volumes:
        - name: kafka-vol
          emptyDir: {}
status: {}
```



**NEW QUESTION: 30**
□□□□ □□□ □□□ □□ 389□□ □□□□ □□□, □□□□□ □□□□ ID□ □□, /candidate/KH77539/files.txt □□□ □□ □□ □□ □□□ □□□ □□□□, □□□□□ □□□□□.

**Answer:**
□□ □□ □□□ □□□ □□□□□ □□□□.

**NEW QUESTION: 31**
□□□□ □□ □□□□ □□□ AppArmor □□□□ □□□□□.
#include <□□□/□□>
□□□ nginx-deny □□□=(attach_disconnected) {
#include <□□□/□□>
□□,
# □□ □□ □□□ □□□□□.
□□ /** in,
}
EOF'
□□□ □□□□□ □□□ □□□□ AppArmor □□□□ □□□□□.
api□□: v1
□□: □□
□□□□□:
□□: □□□□+□□
□□:
□□□□:

- □□: □□□□-□□
□□□: nginx
□□□□□ □□□□□ □□□ □□□□ □□ □□□ □□□ Pod□ □□□□□.
□□: □□□ □□□□ □□ □□□ □□□ □□□.
**Answer:**

```
candidate@cli:~$ kubectl config use-context KSSH00401
Switched to context "KSSH00401".
candidate@cli:~$ ssh kssh00401-worker1
Warning: Permanently added '10.240.86.172' (ECDSA) to the list of known hosts.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

root@kssh00401-worker1:~# head /etc/apparmor.d/nginx_apparmor
#include <tunables/global>

profile nginx-profile-2 flags=(attach_disconnected,mediate_deleted) {
 #include <abstractions/base>
  network inet tcp,
  network inet udp,
  network inet icmp,

  deny network raw,

root@kssh00401-worker1:~# apparmor_parser -q /etc/apparmor.d/nginx_apparmor
root@kssh00401-worker1:~# exit
logout
Connection to 10.240.86.172 closed.
candidate@cli:~$ cat KSSH00401/nginx-pod.yaml
---
apiVersion: v1
kind: Pod
metadata:
  name: nginx-pod
spec:
  containers:
  - name: nginx-pod
```

```
    image: nginx:1.19.0
    ports:
    - containerPort: 80
candidate@cli:~$ vim KSSH00401/nginx-pod.yaml
```

```
---
apiVersion: v1
kind: Pod
metadata:
  name: nginx-pod
  annotations:
    container.apparmor.security.beta.kubernetes.io/nginx-pod: localhost/nginx-pr
spec:
  containers:
  - name: nginx-pod
    image: nginx:1.19.0
    ports:
    - containerPort:
~
```

```
candidate@cli:~$ vim KSSH00401/nginx-pod.yaml
candidate@cli:~$ kubectl create -f KSSH00401/nginx-pod.yaml
pod/nginx-pod created
candidate@cli:~$ cat KSSH00401/nginx-pod.yaml
---
apiVersion: v1
kind: Pod
metadata:
  name: nginx-pod
  annotations:
    container.apparmor.security.beta.kubernetes.io/nginx-pod: localhost/nginx-profile-2
spec:
  containers:
  - name: nginx-pod
    image: nginx:1.19.0
    ports:
    - containerPort: 80
```

**NEW QUESTION: 32**
□□ □□□ □□□□ □□□□/□□ □□□□□ □□□ □ □□□□.
[desk@cli] $ kubectl config use-context qa
□□:
ServiceAccount□ □□ □□□□ Pod□ □□□□ □□□□.
□:
□□ □□□□□□ qa□ backend-qa□□ □□□ □ □□□ □□□ □□□□. □ □□□ □□□ □□□□ □□□ □ □□□ □□□.
□□□ QA □□□ □□□ □□□□□ □□□□□ Pod YAML□ □□□□□.
□□: □□□□□ □□ yaml□ /home/cert_masters/frontend-pod.yaml□□ □□ □ □□□□.
**Answer:**
[desk@cli] $ k create sa backend-qa -n qa
in/backend-qa □□□
[desk@cli] $ k □□ □□□□, □□ □□□ -n qa
qa □□□□□□□□ □□□□ □□ □ □□□□.
[desk@cli] $ k □□ □□□ □□ -n qa --□□□ □□, □□□□□□, □□ □ --□□ □□
# □□□ □□□ □ □□□□
[desk@cli] $ k □□ □□□ □□□ □□ -n qa --□□ □□□ --□□□ □□ qa:□□□-qa
[desk@cli] $ vim /home/cert_masters/frontend-pod.yaml
api□□: v1
□□: □□
□□□□□:
□□: □□□□□
□□:
serviceAccountName: backend-qa # □□□ □□□□□
□□□: nginx
□□: □□□□□
[desk@cli] $ k □□ -f /home/cert_masters/frontend-pod.yaml
□□ □□□
[desk@cli] $ k create sa backend-qa -n qa
serviceaccount/backend-qa □□□
[desk@cli] $ k □□ □□□□, □□ □□□ -n qa
qa □□□□□□□□ □□□□ □□ □ □□□□.
[desk@cli] $ k □□ □□□ □□ -n qa --□□□ □□, □□□□□□, □□ □ --□□ □□ □□.rbac.authorization.k8s.io/backend □□□
[desk@cli] $ k □□ □□□ □□□ □□ -n qa --□□ □□□ --□□□ □□ qa:□□□-qa□□ □□□.rbac.authorization.k8s.io/□□□ □□□
[desk@cli] $ vim /home/cert_masters/frontend-pod.yaml
api□□: v1

□□: □□
□□□□□:
□□: □□□□□
□□:
serviceAccountName: backend-qa # □□□ □□□□□
□□□: nginx
□□: □□□□□
[desk@cli] $ k apply -f /home/cert_masters/frontend-pod.yaml pod/frontend□ □□□□□□□ https://kubernetes.io/docs/tasks/configure-pod-container/configure-service-account/ pod/frontend□ □□□□□□□
[desk@cli] $ k apply -f /home/cert_masters/frontend-pod.yaml pod/frontend□ https://kubernetes.io/docs/tasks/configure-pod-container/configure-service-account/□ □□□□□□□.

**NEW QUESTION: 33**
□□
□ □□□□□ CRI □□□□□ containerd□ □□□□□.
Containerd□ □□ □□□ □□□□ runc□□□. Containerd□ □□ □□□ □□□□ runsc(gVisor)□ □□□□□ □□□□□□□.
□
runsc□□ □□□ □□□ □□□□ □□□□ sandboxed□□ □□□ RuntimeClass□ □□□□.
gVisor□□ □□□□□ □□□□□□ □□□ □□ □□ Pod□ □□□□□□□.


**Answer:**

```
apiVersion: node.k8s.io/v1
kind: RuntimeClass
metadata:
  name: "sandboxed"
handler: "runsc"
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
:wq!
```

```
candidate@cli:~$ kubectl config use-context KSMV00301
Switched to context "KSMV00301".
candidate@cli:~$ cat /home/candidate/KSMV00301/runtime-class.yaml
---
apiVersion: node.k8s.io/v1
kind: RuntimeClass
metadata:
  name: ""
handler: ""
candidate@cli:~$ vim /home/candidate/KSMV00301/runtime-class.yaml
candidate@cli:~$ cat /home/candidate/KSMV00301/runtime-class.yaml
---
apiVersion: node.k8s.io/v1
kind: RuntimeClass
metadata:
  name: "sandboxed"
handler: "runsc"
candidate@cli:~$ kubectl get deployments.apps -n server
NAME        READY   UP-TO-DATE   AVAILABLE   AGE
workload1   1/1     1            1           5h43m
workload2   1/1     1            1           5h43m
workload3   1/1     1            1           5h43m
candidate@cli:~$ kubectl get pods -n server
NAME                         READY   STATUS    RESTARTS   AGE
workload1-6869857dd7-s45rc   1/1     Running   0          5h43m
workload2-d4bd497d5-h44df    1/1     Running   0          5h43m
workload3-8587774495-chm56   1/1     Running   0          5h43m
candidate@cli:~$ kubectl -n server edit deployments.apps workload1
```

```
  template:
    metadata:
      creationTimestamp: null
      labels:
        app: nginx
      name: workload1
    spec:
      runtimeClassName: sandboxed
      containers:
      - image: nginx:1.14.2
        imagePullPolicy: IfNotPresent
        name: workload1
        ports:
        - containerPort: 80
          protocol: TCP
        resources: {}
        terminationMessagePath: /dev/termination-log
        terminationMessagePolicy: File
      dnsPolicy: ClusterFirst
      restartPolicy: Always
      schedulerName: default-scheduler
      securityContext: {}
      terminationGracePeriodSeconds: 30
status:
"/tmp/kubectl-edit-3385772700.yaml"
```

```
NAME                         READY   STATUS    RESTARTS   AGE
workload1-6869857dd7-s45rc   1/1     Running   0          5h44m
workload2-d4bd497d5-h44df    1/1     Running   0          5h44m
workload3-8587774495-chm56   1/1     Running   0          5h44m
candidate@cli:~$ kubectl -n server edit deployments.apps workload1
Edit cancelled, no changes made.
candidate@cli:~$ kubectl get pods -n server
NAME                         READY   STATUS    RESTARTS   AGE
workload1-6869857dd7-s45rc   1/1     Running   0          5h45m
workload2-d4bd497d5-h44df    1/1     Running   0          5h44m
workload3-8587774495-chm56   1/1     Running   0          5h44m
candidate@cli:~$ kubectl -n server edit deployments.apps workload2
Edit cancelled, no changes made.
candidate@cli:~$ kubectl create -f /home/candidate/KSMV00301/runtime-class.yaml
runtimeclass.node.k8s.io/sandboxed created
candidate@cli:~$ kubectl get pods -n server
NAME                         READY   STATUS    RESTARTS   AGE
workload1-6869857dd7-s45rc   1/1     Running   0          5h45m
workload2-d4bd497d5-h44df    1/1     Running   0          5h45m
workload3-8587774495-chm56   1/1     Running   0          5h45m
candidate@cli:~$ kubectl -n server edit deployments.apps workload2
```

```
strategy:
  rollingUpdate:
    maxSurge: 25%
    maxUnavailable: 25%
  type: RollingUpdate
  template:
    metadata:
      creationTimestamp: null
      labels:
        app: nginx
        name: workload2
    spec:
      runtimeClassName: sandboxed
```

```
NAME                          READY   STATUS    RESTARTS   AGE
workload1-6869857dd7-s45rc    1/1     Running   0          5h45m
workload2-d4bd497d5-h44df     1/1     Running   0          5h45m
workload3-8587774495-chm56    1/1     Running   0          5h45m
candidate@cli:~$ kubectl -n server edit deployments.apps workload2
deployment.apps/workload2 edited
candidate@cli:~$ kubectl get pods -n server
NAME                          READY   STATUS    RESTARTS   AGE
workload1-8d8649ff6-wvjtg     1/1     Running   0          15s
workload2-765bdb98c8-wd8cm    1/1     Running   0          4s
workload3-8587774495-chm56    1/1     Running   0          5h45m
candidate@cli:~$ kubectl -n server edit deployments.apps workload3
    app: nginx
  name: workload3
spec:
  runtimeClassName: sandboxed
  containers:
  - image: nginx:1.14.2
    imagePullPolicy: IfNotPresent
    name: workload3
candidate@cli:~$ kubectl -n server edit deployments.apps workload3
deployment.apps/workload3 edited
candidate@cli:~$ kubectl get pods -n server
NAME                          READY   STATUS    RESTARTS   AGE
workload1-8d8649ff6-wvjtg     1/1     Running   0          58s
workload2-765bdb98c8-wd8cm    1/1     Running   0          47s
workload3-76c994bb4d-s4k5x    1/1     Running   0          4s
candidate@cli:~$
```

**NEW QUESTION: 34**

□□□□: scanner □□□ □□: controlplane □□□ □□: worker1

□□ □□□ □□□□ □□□□/□□ □□□□□ □□□ □ □□□□.

[desk@cli] $ kubectl config □□□□ □□□ □□

□□□ □□: Trivy□ □□□ □□□ □ □□□□.

□□: Trivy □□□□ □□□□ □□□□ □□□□ nato □□□□□□□ Pod□□ □□□□ □□□ □□□□ □□ □□□□ □□□□□.

□□□□ □□□ □□□ □□□□ □□ □□□□ □□ □□ □□□□ □□□□ Pod□ □□□□□. Trivy□ □□□□□ □□□ □□□ □□ □□□□ □□□□. □□□ □□ □□□ □□□ □□□□ Trivy□ □□□□□.

**Answer:**

```
candidate@cli:~$ kubectl config use-context KSSC00401
Switched to context "KSSC00401".
```

```
candidate@cli:~$ ssh kssc00401-master
Warning: Permanently added '10.240.86.231' (ECDSA) to the list of known hosts.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

root@kssc00401-master:~# kubectl get pods -n naboo
NAME           READY   STATUS    RESTARTS   AGE
c-3po          1/1     Running   0          6h48m
chewbacca      1/1     Running   0          6h48m
jawas          1/1     Running   0          6h48m
qui-gon-jinn   1/1     Running   0          6h48m
root@kssc00401-master:~# kubectl get pods -n naboo -o name
pod/c-3po
pod/chewbacca
pod/jawas
pod/qui-gon-jinn
root@kssc00401-master:~# for i in $(kubectl get pods -n naboo -o name)
> do
> kubectl get ${i} -o yaml | grep -i image
> done
Error from server (NotFound): pods "c-3po" not found
Error from server (NotFound): pods "chewbacca" not found
Error from server (NotFound): pods "jawas" not found
Error from server (NotFound): pods "qui-gon-jinn" not found
root@kssc00401-master:~# for i in $(kubectl get pods -n naboo -o name); do kubectl -n naboo
get ${i} -o yaml | grep -i image ; done
    image: centos:centos7.9.2009
    imagePullPolicy: Never
    image: centos:centos7.9.2009
    imageID: docker-pullable://centos@sha256:c73f515d06b0fa07bb18d8202035e739a494ce760aa7312
9f60f4bf2bd22b407
    image: photon:3.0
    imagePullPolicy: Never
    image: photon:3.0
    imageID: docker-pullable://photon@sha256:c48d61f0f3ad19215b75e2087cfbe95d7321abb454e4295
a0e6c38f563ece622
    image: alpine:3.7
    imagePullPolicy: Never
    image: alpine:3.7
    imageID: docker-pullable://alpine@sha256:8421d9a84432575381bfabd248f1eb56f3aa21d9d7cd251
1583c68c9b7511d10
    image: amazonlinux:2
    imagePullPolicy: Never
    image: amazonlinux:2
    imageID: docker-pullable://amazonlinux@sha256:246ef631c75ea83005889621119fd5cc9cbb5500e1
93707c38b6c060d597a146
root@kssc00401-master:~# trivy image centos:centos7.9.2009
2022-05-20T15:39:51.733Z        INFO    Need to update DB
2022-05-20T15:39:51.733Z        INFO    Downloading DB...
27.97 MiB / 27.97 MiB [-------------------------------------------------] 100.00% 27.43 MiB p/s 1s
```

```
root@kssc00401-master:~# for i in $(kubectl get pods -n naboo -o name); do kubectl -n naboo
get ${i} -o yaml | grep -i image ; done
    image: centos:centos7.9.2009
    imagePullPolicy: Never
    image: centos:centos7.9.2009
    imageID: docker-pullable://centos@sha256:c73f515d06b0fa07bb18d8202035e739a494ce760aa7312
9f60f4bf2bd22b407
    image: photon:3.0
    imagePullPolicy: Never
    image: photon:3.0
    imageID: docker-pullable://photon@sha256:c48d61f0f3ad19215b75c2087cfbe95d7321abb454e4295
a0e6c38f563ece622
    image: alpine:3.7
    imagePullPolicy: Never
    image: alpine:3.7
    imageID: docker-pullable://alpine@sha256:8421d9a84432575381bfabd248f1eb56f3aa21d9d7cd251
1583c68c9b7511d10
    image: amazonlinux:2
    imagePullPolicy: Never
    image: amazonlinux:2
    imageID: docker-pullable://amazonlinux@sha256:246ef631c75ea83005889621119fd5cc9cbb5500e1
93707c38b6c060d597a146
root@kssc00401-master:~# trivy image photon:3.0
2022-05-20T15:40:18.003Z        INFO    Detected OS: photon
2022-05-20T15:40:18.003Z        INFO    Detecting Photon Linux vulnerabilities...
2022-05-20T15:40:18.005Z        INFO    Number of language-specific files: 0

photon:3.0 (photon 3.0)
=======================
Total: 0 (UNKNOWN: 0, LOW: 0, MEDIUM: 0, HIGH: 0, CRITICAL: 0)
```

```
pod/c-3po
pod/chewbacca
pod/jawas
pod/qui-gon-jinn
root@kssc00401-master:~# kubectl -n naboo pod/c-3po -o yaml | grep image
Error: flags cannot be placed before plugin name: -n
root@kssc00401-master:~# kubectl -n naboo get pod/c-3po -o yaml | grep image
    image: centos:centos7.9.2009
    imagePullPolicy: Never
    image: centos:centos7.9.2009
    imageID: docker-pullable://centos@sha256:c73f515d06b0fa07bb18d8202035e739a494ce760aa731
9f60f4bf2bd22b407
root@kssc00401-master:~# kubectl -n naboo delete pod/c-3po
pod "c-3po" deleted
root@kssc00401-master:~# kubectl -n naboo delete pod/jawas
pod "jawas" deleted
```

```
root@kssc00401-master:~# history
    1  kubectl get pods -n naboo
    2  kubectl get pods -n naboo -o name
    3  for i in $(kubectl get pods -n naboo -o name); do kubectl get ${i} -o yaml | grep -i
image ; done
    4  for i in $(kubectl get pods -n naboo -o name); do kubectl -n naboo get ${i} -o yaml |
 grep -i image ; done
    5  trivy image centos:centos7.9.2009
    6  for i in $(kubectl get pods -n naboo -o name); do kubectl -n naboo get ${i} -o yaml |
 grep -i image ; done
    7  trivy image photon:3.0
    8  for i in $(kubectl get pods -n naboo -o name); do kubectl -n naboo get ${i} -o yaml |
 grep -i image ; done
    9  trivy image alpine:3.7
   10  for i in $(kubectl get pods -n naboo -o name); do kubectl -n naboo get ${i} -o yaml |
 grep -i image ; done
   11  trivy image amazonlinux:2
   12  kubectl get pods -n naboo -o name
   13  kubectl -n naboo pod/c-3po -o yaml | grep image
   14  kubectl -n naboo get pod/c-3po -o yaml | grep image
   15  kubectl -n naboo delete pod/c-3po
   16  kubectl -n naboo delete pod/jawas
   17  history
root@kssc00401-master:~#
```



**NEW QUESTION: 35**

□□□□□

□□□□ □□ □□□□ □□□ AppArmor □□□□ □□□□□.

#include <□□□/□□>

□□□ nginx-deny □□□=(attach_disconnected) {

#include <□□□/□□>
□□,
# □□ □□ □□□ □□□□□.
□□ /** in,
}
EOF'
□□□ □□□□□ □□□ □□□□ AppArmor □□□□ □□□□□.
api□□: v1
□□: □□
□□□□□:
□□: □□□□□□□
□□:
□□□□:
- □□: □□□□□□□
□□□: nginx
□□□□□ □□□□□ □□□ □□□□ □□ □□□ □□□ Pod□ □□□□□.
□□: □□□ □□□□ □□ □□□ □□□ □□□.
**Answer:**
□□ □□ □□□□ □□□□□.

**NEW QUESTION: 36**
etcd□ □□□ □□□ □□□□ □□□□. □□ □□ etcdctl □□ □□□□□ □□□□ □□ □□ □□ □ □□□□. ETCDCTL_API=3 etcdctl
get /registry/secrets/default/cks-secret --cacert="ca.crt" --cert="server.crt" --key="server.key" □□


□□□ □□□ □□□□ □□□ AES-CBC □ ID□ □□□□ □□□ □□□ □□□□ □□□□□□ □□□□ □□ □□ □□ □□□□ □□□□□ □□ □□□ □ □ □□□ □□□□□□ □□□.
**Answer:**
ETCD □□ □□□□ etcdctl □□□ □□□□□ □□ □□□ □ □□□□.
ETCD □□□ □□□ □□□ /registry/secrets/$namespace/$secret □□□ □□□□□.
□□ □□□ □□□□ □□ ETCD □□□□□ □□□□□□□ □□□ □□□ □ □□□□.
# ETCDCTL_API=3 etcdctl get /registry/secrets/default/secret1 [...] | hexdump -C

**NEW QUESTION: 37**
□□ □□□ □□□□ □□□□/□□ □□□□□ □□□ □ □□□□. [desk@cli] $ kubectl config use-context dev □□□□: kubeadm□□ □□□ □□□□□ □□
CIS □□□□ □□□ □□□□ □□□□ □ □□ □□□ □□□□□□. □□: □□□ □□ □□ □□□ □□□□ □□□ □□ □□ □□□ □□ □□□□ □ □□□ □

□□□□ □□□. API □□□□ □□□ □□ □□ □□□ □□ □□□□□. 1.2.7 authorization-mode □□□ AlwaysAllow FAIL□ □□□□ □□ 1.2.8 authorization-mode □□□ Node FAIL□ □□□ 1.2.7 authorization-mode □□□ RBAC FAIL□ □□□ Kubelet□□ □□□ □□ □□ □□□ □□ □□□□□. 4.2.1 anonymous-auth □□□ false FAIL□ □□□□□□ □□□□□. 4.2.2 authorization-mode □□□ AlwaysAllow FAIL□ □□□□ □□(□□□ □□ Webhook autumn/authz □□) etcd□□ □□□ □□ □□ □□□ □□ □□□□□. 2.2 client-cert-auth □□□ true□ □□□□□□ □□□□□.

**Answer:**

worker1 $ vim /var/lib/kubelet/config.yaml

□□□:

□□□□: true # □□□ □□□□□

enabled: false # □□□□ □□

□□ □□:

□□: AlwaysAllow # □□

□□: Webhook #□□□□ □□

worker1 $ systemctl restart kubelet. # kubelet □□□ □□ □□□□□ master1□ ssh□ □□□□□. master1 $ vim /etc/kubernetes/manifests/kube-apiserver.yaml - --authorization-mode=Node,RBAC master1 $ vim /etc/kubernetes/manifests/etcd.yaml - --client-cert-auth=true □□ worker1□ ssh□ □□□□□. worker1 $ vim /var/lib/kubelet/config.yaml apiVersion: kubelet.config.k8s.io/v1beta1 authentication:

□□□:

□□□□: true # □□□ □□□□□

enabled: false # □□□□ □□

□□:

□□TTL: 0□

□□□□: true

x509:

□□□□□CA□□: /etc/kubernetes/pki/ca.crt

□□ □□:

□□: AlwaysAllow # □□

□□: Webhook #□□□□ □□

□□:

□□AuthorizedTTL: 0□

□□UnauthorizedTTL: 0s

cgroupDriver: systemd

□□□□DNS:

- 10.96.0.10

clusterDomain: cluster.local

cpuManagerReconcilePeriod: 0□

evictionPressureTransitionPeriod: 0□

□□ □□ □□: 0□

healthzBind□□: 127.0.0.1

healthz□□: 10248

http□□□□: 0□

imageMinimumGCAge: 0□

□□: KubeletConfiguration

□□: {}
nodeStatusReportFrequency: 0s
□□ □□ □□□□ □□: 0□
resolvConf: /run/systemd/resolve/resolv.conf
rotateCertificates: true
□□□□□□□□□: 0□
□□PodPath: /etc/kubernetes/manifests
□□□□ □□ □□ □□ □□: 0□
□□□ □□: 0□
volumeStatsAggPeriod: 0□
worker1 $ systemctl restart kubelet. # kubelet □□□ □□ □□□□□ ssh□ master1□ □□□□ master1 $ vim /etc/kubernetes/manifests/kube-apiserver.yaml

```yaml
apiVersion: v1
kind: Pod
metadata:
  annotations:
    kubeadm.kubernetes.io/kube-apiserver.advertise-address.endpoint: 172.17.0.22:6443
  labels:
    component: kube-apiserver
    tier: control-plane
  name: kube-apiserver
  namespace: kube-system
spec:
  containers:
  - command:
    - kube-apiserver
    - --advertise-address=172.17.0.22
    - --allow-privileged=true
#     - --authorization-mode=AlwaysAllow  # Delete This
    - --authorization-mode=Node,RBAC    # Replace by this line
    - --client-ca-file=/etc/kubernetes/pki/ca.crt
    - --enable-admission-plugins=NodeRestriction
    - --enable-bootstrap-token-auth=true
    - --etcd-cafile=/etc/kubernetes/pki/etcd/ca.crt
    - --etcd-certfile=/etc/kubernetes/pki/apiserver-etcd-client.crt
    - --etcd-keyfile=/etc/kubernetes/pki/apiserver-etcd-client.key
    - --etcd-servers=https://127.0.0.1:2379
    - --insecure-port=0
```

master1 $ vim /etc/kubernetes/manifests/etcd.yaml

```
apiVersion: v1
kind: Pod
metadata:
  annotations:
    kubeadm.kubernetes.io/etcd.advertise-client-urls: https://172.17.0.29:2379
  creationTimestamp: null
  labels:
    component: etcd
    tier: control-plane
  name: etcd
  namespace: kube-system
spec:
  containers:
  - command:
    - etcd
    - --advertise-client-urls=https://172.17.0.29:2379
    - --cert-file=/etc/kubernetes/pki/etcd/server.crt
    - --client-cert-auth=true  #Add this line
    - --data-dir=/var/lib/etcd
    - --initial-advertise-peer-urls=https://172.17.0.29:2380
    - --initial-cluster=controlplane=https://172.17.0.29:2380
    - --key-file=/etc/kubernetes/pki/etcd/server.key
    - --listen-client-urls=https://127.0.0.1:2379,https://172.17.0.29:2379
    - --listen-metrics-urls=http://127.0.0.1:2381
    - --listen-peer-urls=https://172.17.0.29:2380
    - --name=controlplane
    - --peer-cert-file=/etc/kubernetes/pki/etcd/peer.crt
    - --peer-client-cert-auth=true
    - --peer-key-file=/etc/kubernetes/pki/etcd/peer.key
    - --peer-trusted-ca-file=/etc/kubernetes/pki/etcd/ca.crt
    - --snapshot-count=10000
    - --trusted-ca-file=/etc/kubernetes/pki/etcd/ca.crt
    image: k8s.gcr.io/etcd:3.4.9-1
    imagePullPolicy: IfNotPresent
```