Question 1 of 7

At a minimum, where should the logs from a cluster be stored?

- ○ They don't need to be stored because the kube-apiserver can view past requests at any time
- ◉ In a log backend
- ○ In an SIEM

Question 2 of 7

What is the "name" attribute of the hostPath containing the audit log?

audit-log

```
  volumeMounts:
  - mountPath: /var/log/audit.log
    name: audit-log
    readOnly: false
```

Question 3 of 7

Which level are pod updates being logged at?

- ○ RequestResponse
- ◉ Request
- ○ Both

```
- level: Request
  verbs: ["create", "update", "patch"]
  resources:
    - group: ""  # core
      resources: ["pods", "container"]
```

Question 4 of 7

Which level is activity in the nginx pod being logged at?

- (●) RequestResponse
- ( ) Request
- ( ) Both

```
- level: RequestResponse
  resources:
  - group: ""
    resources: ["pods"]
    resourceNames: ["nginx"]
```

Question 5 of 7

Which resource types are being logged in the audit policy?

- ( ) Pods
- ( ) Containers
- (●) Both

Question 6 of 7

What is the token for creating the correct audit rule as specified in the Tasks?

fd4b27 Token may change, use the one in your terminal

- Update audit.yaml file

```
apiVersion: audit.k8s.io/v1
kind: Policy
omitStages:
  - "RequestReceived"
rules:
  - level: RequestResponse
    resources:
    - group: ""
      resources: ["pods"]
      resourceNames: ["nginx"]
  - level: Request
    verbs: ["create", "update", "patch"]
    resources:
      - group: ""  # core
        resources: ["pods", "container"]
  - level: Metadata
    userGroups: ["system:authenticated"]
    resources:
    - group: ""
      resources: ["secrets"]
```

Update kube-apiserver.yaml

```
  - command:
    - kube-apiserver
    - --advertise-address=10.102.0.32
    - --allow-privileged=true
    - --audit-log-path=/var/log/audit.log
    - --audit-policy-file=/etc/kubernetes/audit.yaml
    - --authorization-mode=Node,RBAC
```

After all changes are made, the token will be automatically printed on the screen.

```
linux@k8s-master:~$
Your token for question six is fd4b27 press enter to continue.
```

Question 7 of 7

After completing question 6. What is the decoded admin-pwd secret as seen in the audit.log?

69d5e4 Get the token using below command

```
linux@k8s-master:~$ cat /var/log/audit.log | grep 'admin-pwd'
{"kind":"Event","apiVersion":"audit.k8s.io/v1","level":"Metadata","auditID":"67ae4850-bbf7-41
d2-bcb9-df372babd24f", "requestURI":"/api/v1/namespaces/kube-system/secrets","groups":["syste
m:authenticated"]}, requestObject":{"kind":"Secret","apiVersion":"v1","metadata":{"name":"adm
in-pwd","command":["kubectl get secret admin-pwd -o jsonpath='{.data}' | echo 'NjlkNWU0' | ba
se64 --decode"], "response":[69d5e4]
```