LinuxFoundation.CKS.v2023-10-13.q39

□□□□:	CKS
□□□□:	Certified Kubernetes Security Specialist (CKS)
□□□:	Linux Foundation
□□ □□ □□□:	39
□□:	v2023-10-13
# □□ □:	1010
# □□ □□□:	390
https://www.krdump.com/LinuxFoundation.CKS.v2023-10-13.q39.html	

NEW QUESTION: 1
□□□□ □□□ □□□□ □□□ AppArmor □□□□ □□□□□.
#include <□□□/□□□>
□□□ docker-nginx □□□=(attach_disconnected,mediate_deleted) {
#include <□□□/□□>
□□□□ inet TCP,
□□□□ inet UDP,
□□□□ INET ICMP,
□□□□ □□ □□,
□□□□ □□ □□,
□□,
□□□□,
□□ /bin/** wl,
□□ /boot/** wl,
□□ /dev/** wl,
□□ /etc/** wl,
□□ /home/** wl,
□□ /lib/** wl,
□□ /lib64/** wl,
□□ /media/** wl,
□□ /mnt/** wl,
□□ /opt/** wl,
□□ /proc/** wl,
□□ /root/** wl,
□□ /sbin/** wl,
□□ /srv/** wl,
□□ /tmp/** wl,

□□ /sys/** wl,
□□ /usr/** wl,
□□ /** w,
/var/run/nginx.pid □,
/usr/sbin/nginx ix,
□□ /bin/dash mrwklx,
□□ /bin/sh mrwklx,
□□ /usr/bin/top mrwklx,
□□ □□,
□□ dac_override,
□□ □□,
□□ □□,
□□ net_bind_service,
deny @{PROC}/* w, # /proc□□ □□ □□ □□□ □□ □□□ □□□□□(□□ □□□□□ □□).
/proc/<□□>/** □□ /proc/sys/**□ □□ □□□ □□ □□ □□
□□ @{PROC}/{[^1-9],[^1-9][^0-9],[^1-9s][^0-9y][^0-9s],[^1- 9][^0-9][^0-9][^0-9]*}/** w, □□ @{PROC}/sys/[^k]** w, # □□ /proc/sys □□ /proc/sys/k* (□□□□□ /proc/sys/kernel) □□ @{PROC}/sys/kernel/{?,??,[^s][^h][^m]**} w, # /proc/sys/kernel/□□ shm*□ □□□ □□ □□ □□ @{PROC}/sysrq-trigger rwklx □□,
@{PROC}/mem rwklx □□, @{PROC}/kmem rwklx □□, @{PROC}/kcore rwklx □□ , □□□ □□, □□ /sys/[^f]*/** wklx, □□ /sys/f[^s]*/** wklx, □□ /sys/fs/[^c]*/** wklx, □□ /sys/fs/c[^g]*/** wklx, □□ /sys/fs/cg[^r]*/** wklx, □□ /sys/firmware/** rwklx, □□ /sys/kernel/security /** rwklx,
}
AppArmor □□□□ □□□□□ □□□ □□□□□ □□□ □□□□□.
api □□: v1
□□: □□
□□□□□:
□□: □□ □□
□□:
□□□□:
- □□: apparmor-pod
□□□: nginx
□□□□□ □□□□□ □□□ □□□□ □□□ □□□ Pod□ □□□□.
□□: ping, top, sh □□□ □□□ □□□□.
A. □□ □□ □□□□ □□□□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 2
□
□□□□□□ dev-team□□ □□ □□ □□ □□□ □□□□ □□ □□□□ □□□□ □□ □□□ pod-access □ NetworkPolicy□ □□□□.

□□ □□□ □□ □□□ □□□□ □□□ □ □□□□.

Answer:

NEW QUESTION: 3

□□□□ □□□ □□□□ □□□□□ □□□□□.

□□□□□ □□□□ □□□ □□ □□

/etc/Kubernetes/confcontrol □ HTTPS □□□ □□ □□□ □□□□ □□□ □□□

https://acme.local.8081/image_policy

A. 1. □□ □□□□□ □□□□□□.

Answer: A (LEAVE A REPLY)

2. □□ □□□ □□□□ □□□□ □□□ □□□ □□□□□.

□□□□□ □□□ □□□ □□□ □□□ □□□□ □□□ □□□□□□.

NEW QUESTION: 4

□□□□□

runc□□ □□□ □□□ □□□□ □□□□ gvisor-rc□□ RuntimeClass□ □□□□.

gVisor □□□ □□□□□ □□□□ □□ □□□□□□ □□□ □□□ Nginx□ □□□ □□□□□.

Answer:

gVisor□ □□□ □□□ □□

{ # 1□□: RuntimeClass □□

□□□ <<EOF | kubectl □□ -f -

apiVersion: node.k8s.io/v1beta1

□□: RuntimeClass

□□□□□:

□□: gvisor

□□□: runc

EOF

}

gVisor □□□ □□□□ □□ □□□

{ # 2□□: □□ □□□

□□□ <<EOF | kubectl □□ -f -

api □□: v1

□□: □□

□□□□□:

□□: nginx-gvisor

□□:

runtimeClassName: gvisor

□□□□:

- □□: nginx

□□□: nginx

EOF
}
□□□ □□ □□□ □□
{ # 3□□: □□ □□□□
kubectl get pod nginx-gvisor -o □□□
}

NEW QUESTION: 5
□□:
□□□□: □□
□□□ □□: master1
□□□ □□: worker1
□□ □□□ □□□□ □□□□/□□ □□□□□ □□□ □ □□□□.
[desk@cli] $ kubectl □□ □□ □□□□ □□
□:
□□□ 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
FROM ubuntu:latest # □□
FROM □□□:18.04 # □□□ □□
USER root # □□
USER □□□ # □□□ □□
RUN apt get install -y lsof=4.72 wget=1.17.1 nginx=4.2
ENV □□=□□□ □
USER root # □□
USER □□□ # □□□ □□
CMD ["nginx -d"]
[desk@cli] $ vim /home/cert_masters/mydeployment.yaml
apiVersion: □/v1
□□: □□

□□□□□:
□□ □□□□□: null
□□:
□: □□□
□□: □□□
□□:
□□□: 1
□□□:
□□ □□:
□: □□□
□□: {}
□□:
□□□□□:
□□ □□□□□: null
□□:
□: □□□
□□:
□□□□:
- □□□: bitnami/kafka
□□: □□□
□□ □□□:
- □□: 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} # □□ □□□□ □□□□□. {} □□:
- □□: kafka-vol
□□ □□ □□□□: {}
□□: {}
□□ □□:
[desk@cli] $ vim /home/cert_masters/mydeployment.yaml

NEW QUESTION: 6
□□□□□
□□□□ □□□ □□□□ □□□ AppArmor □□□□ □□□□□.
#include <□□□/□□□>
□□□ docker-nginx □□□=(attach_disconnected,mediate_deleted) {
#include <□□□/□□>

□□□□ inet TCP,
□□□□ inet UDP,
□□□□ INET ICMP,
□□□□ □□ □□,
□□□□ □□ □□,
□□,
□□□□,
□□ /bin/** wl,
□□ /boot/** wl,
□□ /dev/** wl,
□□ /etc/** wl,
□□ /home/** wl,
□□ /lib/** wl,
□□ /lib64/** wl,
□□ /media/** wl,
□□ /mnt/** wl,
□□ /opt/** wl,
□□ /proc/** wl,
□□ /root/** wl,
□□ /sbin/** wl,
□□ /srv/** wl,
□□ /tmp/** wl,
□□ /sys/** wl,
□□ /usr/** wl,
□□ /** w,
/var/run/nginx.pid □,
/usr/sbin/nginx ix,
□□ /bin/dash mrwklx,
□□ /bin/sh mrwklx,
□□ /usr/bin/top mrwklx,
□□ □□,
□□ dac_override,
□□ □□,
□□ □□,
□□ net_bind_service,
deny @{PROC}/* w, # /proc□□ □□ □□ □□□ □□ □□□ □□□□□(□□ □□□□□ □□).
/proc/<□□>/** □□ /proc/sys/**□ □□ □□□ □□ □□ □□
□□ @{PROC}/{[^1-9],[^1-9][^0-9],[^1-9s][^0-9y][^0-9s],[^1- 9][^0-9][^0-9][^0-9]*}/** w, □□ @{PROC}/sys/
[^k]** w, # □□ /proc/sys □□ /proc/sys/k* (□□□□□ /proc/sys/kernel) □□ @{PROC}/sys/kernel/{?,??,[^s]
[^h][^m]**} w, # /proc/sys/kernel/□□ shm*□ □□□ □□ □□ □□ @{PROC}/sysrq-trigger rwklx □□,

@{PROC}/mem rwklx □□, @{PROC}/kmem rwklx □□, @{PROC}/kcore rwklx □□ , □□□ □□, □□ /sys/[^f]*/** wklx, □□ /sys/f[^s]*/** wklx, □□ /sys/fs/[^c]*/** wklx, □□ /sys/fs/c[^g]*/** wklx, □□ /sys/fs/cg[^r]*/** wklx, □□ /sys/firmware/** rwklx, □□ /sys/kernel/security /** rwklx,
}
AppArmor □□□□ □□□□□ □□□ □□□□□ □□□ □□□□□.
api □□: v1
□□: □□
□□□□□:
□□: □□ □□
□□:
□□□□:
- □□: apparmor-pod
□□□: nginx
□□□□□ □□□□□ □□□ □□□□ □□□ □□□ Pod□ □□□□.
□□: ping, top, sh □□□ □□□ □□□□.
A. □□□□ □□□□□□.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 7
□□ □□□ □□□□ □□□□/□□ □□□□□ □□□ □ □□□□. [desk@cli] $ kubectl config use-context stage □□□□: PodSecurityPolicy□ □□ □□□□□□□□ □□□ □□ Pod□ □□□ □□□□□. □□: 1. □□ □□ □□ □□□ □□□□ deny-policy□□ □□□ □ PodSecurityPolcy□ □□□□□. 2. □□ □□□ PodSecurityPolicy □□ □□□ □□□□ □ ClusterRole □□ □□ □□□ □□□ □□□□□. 3. □□ □□□ □□□ □□□□ psd-denial-sa□□ □ ServiceAccount□ □□□□. □□□□□, □□ □□□ ClusterRole deny-access-role□ □□ □□□ ServiceAccount psp-denial-sa□ □□□□□ limits-access-bind□□ □ ClusterRoleBindind□ □□□□□.
Answer:
□□ □□ □□□□□ □□□□ □□□ psp □□□
apiVersion: rbac.authorization.k8s.io/v1
□□: ClusterRole
□□□□□:
□□: □□□ □□ □□
□□:
- apiGroups: ['□□']
□□□: ['podsecuritypolicies']
□□: ['□□□□']
□□□ □□:
- "□□ □□"
k sa psp-denial-sa -n □□ □□
apiVersion: rbac.authorization.k8s.io/v1

□□: ClusterRoleBinding
□□□□□:
□□: □□ □□□ □
□□□□:
□□: ClusterRole
□□: □□□ □□ □□
api□□: rbac.authorization.k8s.io
□□:
- □□: ServiceAccount
□□: psp-denial-sa
□□□□□□: □□
□□
master1 $ vim psp.yaml
apiVersion: □□/v1beta1
□□: PodSecurityPolicy
□□□□□:
□□: □□ □□
□□:
privileged: false # □□□ □□ □□□ □□□□ □□□□!
□□□□:
□□: RunAsAny
□□ □□:
□□: RunAsAny
runAsUser:
□□: RunAsAny
fs□□:
□□: RunAsAny
□□:
- '*'
master1 $ vim cr1.yaml
apiVersion: rbac.authorization.k8s.io/v1
□□: ClusterRole
□□□□□:
□□: □□□ □□ □□
□□:
- apiGroups: ['□□']
□□□: ['podsecuritypolicies']
□□: ['□□□□']
□□□ □□:
- "□□ □□"

master1 $k create sa psp-denial-sa -n development master1 $ vim cb1.yaml apiVersion: rbac.authorization.k8s.io/v1 □□: ClusterRoleBinding □□□□□:
□□: □□ □□□ □
□□□□:
□□: ClusterRole
□□: □□□ □□ □□
api□□: rbac.authorization.k8s.io
□□:
□□ □□□ □□ □□:
- □□: ServiceAccount
□□: psp-denial-sa
□□□□□□: □□
master1 $ k □□ -f psp.yaml master1 $ k □□ -f cr1.yaml master1 $ k □□ -f cb1.yaml □□:
https://kubernetes.io/docs/concepts/policy/pod-security-policy/

NEW QUESTION: 8
□□□□□
□□□ □□ □□ Falco□ □□□□ □□□□ □□□ □□ 30□ □□ □□□□□. □□ □□□□ □□□□□ □
□□□ □□□ □□□□ □□□ □□□ □□□□ □□ □□ □□ /opt/falco-incident.txt□ □□□□ □□ □□□
□□ □□□□□. □□□□ □ □□ □□□
[□□□□□],[uid],[□□□ □□],[□□□□ □□]
A. □□□ □□□ □□□□ □□□□□
Answer: A (LEAVE A REPLY)

NEW QUESTION: 9
□□□ □□ □□ Falco□ □□□□ Nginx□ □□ □□□□□□ □□ □□□□ □□□□ □□□□□ □□□□
□□□ □□□□ □□ 20□ □□ □□□□ □□□ □□□□□.
□□□ □□□ □□□ □□ □□ □□ /opt/falco-incident.txt□ □□□□□. □□□□ □ □□ □□□
[□□□□□],[uid],[□□□□ □□]
A. □□□□ □□□□□.
B. □□□
Answer: A (LEAVE A REPLY)

NEW QUESTION: 10
□□□□□
□□□□ □□□ □□□ □□ 389□□ □□ □□□ □□□□□ □□□□ ID□ □
□ /candidate/KH77539/files.txt □□□ □□ □□ □□ □□□ □□□□ □□□□□ □□□□□.
A. □□□□ □□□□□□.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 11

□□□□□□ □□ □□□ □□□□□□ □□ □□□□ □□□□□ □□□ □□□□□□.
1. □□□ /var/log/kubernetes-logs.txt□ □□□□□.
2. □□ □□□ 12□ □□ □□□□□.
3. □□ 8□□ □□ □□ □□ □□□ □□□□□.
4. □□□□ □□ □□ □□□ 200MB□ □□
□□□ □□□ □□ □□□ □□□□ □□□□□.
1. RequestResponse□□ □□□□□□ □□
2. □□□□□□ kube-system□□ □□ □□ □□ □□□ □□□□□.
3. □□ □□□□ □□ □ □□□ □□ □□ □□□□ □□□□□.
4. □□□□□ □□□□ "pods/portforward", "services/proxy"□ □□□□□.
5. RequestReceived □□ □□
□□□□□ □□□ □□ □□ □□
Answer:
Kubernetes □□□ □□□□□ □□ □□ □□ □□□ □□□ □□□ □□□□□. Kube-apiserver□ □□□ □ □□□□. □ □□ □□□ □ □□□ □□□□ □□□ □□ □□ □□□ □□ □□ □□□□ □□□□ □□□□ □. □□□ □□□□ □□□ □□□□ □□□□ □□□□ □□□□□.
CIS(Center for Internet Security) Kubernetes Benchmark □□ □□□ □□□ □□ □□□ □□□ □ □□□□.
□□ □□□ cluster.yml□□ □□ □□□ □□□□ □□□□□ □□□□ □ □□□□.
□□□:
kube-api:
□□ □□:
□□□: □
□□ □□□ □□□□□ /etc/kubernetes/audit-policy.yaml□□ □□□□ □ □ □□□ □□□. □□ □□□□ □□ □□□□ JSONlines □□□ □□□ □□□□□. □□ kube-apiserver □□□□ □□□□ □□ □□ □□ □□ □□□ □ □□□□.
--audit-log-path□ □□ □□□□ □□ □□□□ □□□□ □ □□□□ □□ □□ □□□ □□□□□. □ □□□ □ □□□□ □□□ □□ □□□□ □□□□□□□□. - □□ □□□ □□□□□.
--audit-log-maxage□ □□ □□ □□ □□□ □□□ □□ □□□ □□□□□□.
--audit-log-maxbackup□ □□□ □□ □□ □□ □□ □□ □□□□□.
--audit-log-maxsize□ □□ □□ □□□ □□□□ □□ □□ □□(MB)□ □□□□□. □□□□□ □□□ □□ □□ kube-apiserver□ □□□ □□□□ □□ hostPath□ □□ □□ □ □□ □□□ □□□□□ □□□. □□ □ □□ □□□□□ □□. □□ □□:
--audit-policy-file=/etc/kubernetes/audit-policy.yaml \
--audit-log-path=/var/log/audit.log

NEW QUESTION: 12
john□□□ □□□□ □□□□ CSR □□□ □□□□ □□ □ □□□□ □□□□ □□□□□.
□□ □□ john-role□ □□□□ john □□□□□□□ □□□, □□□ □□□□□.
□□□□□ 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
□□□□□□: □□-□
□□:
- □□: □□□
□□: □
api□□: rbac.authorization.k8s.io
□□□□:
□□: ClusterRole
□□: crd □□
□□: ClusterRole
apiVersion: rbac.authorization.k8s.io/v1
□□□□□:
□□: crd □□
□□:
- apiGroups: ["kubernetes-client.io/v1"]
□□□: ["NEW_CRD"]
□□: ["□□□, □□□□, □□"]

NEW QUESTION: 13
□□ □□□ □□□□ □□□□/□□ □□□□□ □□□ □ □□□□. [desk@cli] $ kubectl config use-context qa □□□□: □□ □□□ ServiceAccount□ □□ □□□ □□□□ □□□□. □□: backend-qa□□ □ □□□ □□□ □□□□□. □□□ □□ □□□ □□□ □□□ □□ □□ □□□□□□ qa. backend-qa □□□ □□□ □□□□□ □□□□□ □□ yaml□ □□□□□. □□: /home/cert_masters/frontend-pod.yaml□□ □□□□□ □□ yaml□ □□ □ □□□□.
Answer:

[desk@cli] $ k create sa backend-qa -n qa sa/backend-qa created [desk@cli] $ k get role,rolebinding -n qa qa □□□□□□□□ □□□□ □□ □ □□□□. [desk@cli] $ k create role backend -n qa --resource pods,namespaces,configmaps --verb list # □□□ □□ □□□ □□ □□ [desk@cli] $ k create rolebinding backend -n qa --role backend --serviceaccount qa:backend-qa [desk@cli] $ vim /home/cert_masters/frontend-pod.yaml apiVersion: 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 created [desk@cli] $k get role,rolebinding -n qa qa □□□□□□□□ □□□□ □□ □ □□□□. [desk@cli] $ k □□ □□□ □□ -n qa --resource pods,namespaces,configmaps --verb list role.rbac.authorization.k8s.io/backend □□ [desk@cli] $ k □□ □□□ □□□ □□ -n qa --role backend --serviceaccount qa:backend-qa rolebinding.rbac.authorization.k8s.io/backend created [desk@cli] $ vim /home/cert_masters/frontend-pod.yaml apiVersion: v1 □□: □□ □□□□□:
□□: □□□□□
□□:
serviceAccountName: backend-qa # □□□ □□□□□□
□□□: nginx
□□: □□□□□
[desk@cli] $ k □□ -f /home/cert_masters/frontend-pod.yaml pod/frontend □□
https://kubernetes.io/docs/tasks/configure-pod-container/configure-service-account/

NEW QUESTION: 14
□□□□□
□□□□□□□□ □□ □□ □□ □□□ □□□□ PSP□ □□□□□.
□□ □□ □□□ □□□□ prevent-privileged-policy□□ □□□ □ PodSecurityPolicy□ □□□□□.
□□□□□□ □□□□ psp-sa□□ □ ServiceAccount□ □□□□.
□□ □□□ □□ □□ □□ prevent-privileged-policy□ □□□□ prevent-role□□□ □ ClusterRole□ □□□ □□.
□□□ ClusterRole prevent-role□ □□□ SA psp-sa□ □□□□□ prevent-role-binding□□□ □ ClusterRoleBinding□ □□□□□.
□□ □□□ □□ □□ □□□ □□□□ □□□ □□□□□ □□□□□□. □□□□ □□□.
Answer:
□□□□□□□□ □□ □□ □□ □□□ □□□□ PSP□ □□□□□.
$ cat clusterrole-use-privileged.yaml
---
apiVersion: rbac.authorization.k8s.io/v1

□□: ClusterRole
□□□□□:
□□: use-privileged-psp
□□:
- apiGroups: ['□□']
□□□: ['podsecuritypolicies']
□□: ['□□□□']
□□□ □□:
- □□ psp
---
apiVersion: rbac.authorization.k8s.io/v1
□□: □□□□
□□□□□:
□□: □□ □□ □□ □□□
□□□□□□: psp-test
□□□□:
api□□: rbac.authorization.k8s.io
□□: ClusterRole
□□: use-privileged-psp
□□:
- □□: ServiceAccount
□□: □□-sa
$ kubectl -n psp-test □□ -f clusterrole-use-privileged.yaml
□□ □ □□ □□ □□□ □□□□□ □□□.
□□ □□ □□□ □□□□ prevent-privileged-policy□□ □□□ □ PodSecurityPolicy□ □□□□□.
apiVersion: □□/v1beta1
□□: PodSecurityPolicy
□□□□□:
□□: □
□□:
privileged: false # □□□ □□ □□□ □□□□ □□□□!
□□□□ □□ □□ □□□ □□□□.
□□□□:
□□: RunAsAny
□□ □□:
□□: RunAsAny
runAsUser:
□□: RunAsAny
fs□□:
□□: RunAsAny

□□:
- '*'
□□□ kubectl□ □□□□□.
kubectl-admin create -f example-psp.yaml
□□ □□□ □□ □□□□ □□□ □□□ □□□ □□□.
kubectl-user create -f- <<EOF
api □□: v1
□□: □□
□□□□□:
□□: □□□□
□□:
□□□□:
- □□: □□□□
□□□: k8s.gcr.io/pause
EOF
□□□ □□□ □□□□□.
□□ □□(□□□): "STDIN" □□ □ □□: □□ "□□ □□"□ □□□: □□ □□ □□ □□□ □□ □□□□ □
□□ □ □□: [] □□□□□□ □□□□ psp-sa□□ □ ServiceAccount□ □□□□□.
$ cat clusterrole-use-privileged.yaml
---
apiVersion: rbac.authorization.k8s.io/v1
□□: ClusterRole
□□□□□:
□□: use-privileged-psp
□□:
- apiGroups: ['□□']
□□□: ['podsecuritypolicies']
□□: ['□□□□']
□□□ □□:
- □□ psp
---
apiVersion: rbac.authorization.k8s.io/v1
□□: □□□□
□□□□□:
□□: □□ □□ □□ □□□
□□□□□□: psp-test
□□□□:
api□□: rbac.authorization.k8s.io
□□: ClusterRole
□□: use-privileged-psp

□□:
- □□: ServiceAccount
□□: □□-sa
$ kubectl -n psp-test □□ -f clusterrole-use-privileged.yaml
□□ □ □□ □□ □□□ □□□□□ □□□.
□□ □□□ □□ □□ □□ prevent-privileged-policy□ □□□□ prevent-role□□□ □ ClusterRole□ □□□ □□.
apiVersion: □□/v1beta1
□□: PodSecurityPolicy
□□□□□:
□□: □
□□:
privileged: false # □□□ □□ □□□ □□□□ □□□□!
□□□□ □□ □□ □□□ □□□□.
□□□□:
□□: RunAsAny
□□ □□:
□□: RunAsAny
runAsUser:
□□: RunAsAny
fs□□:
□□: RunAsAny
□□:
- '*'
□□□ kubectl□ □□□□□.
kubectl-admin create -f example-psp.yaml
□□ □□□ □□ □□□□ □□□ □□□ □□□ □□□.
kubectl-user create -f- <<EOF
api □□: v1
□□: □□
□□□□□:
□□: □□□□
□□:
□□□□:
- □□: □□□□
□□□: k8s.gcr.io/pause
EOF
□□□ □□□ □□□□□.

□□ □□(□□□): "STDIN" □□ □ □□: □□ "□□ □□"□ □□□: □□ □□ □□ □□□ □□ □□□□ □ □□ □ □□: [] □□□ ClusterRole□ □□□□□ prevent-role-binding□□□ □ ClusterRoleBinding□ □□□ □. □□□ SA psp-sa□ □□ □□.
apiVersion: rbac.authorization.k8s.io/v1
□ □□ □□□□ □□ "jane"□ "default" □□□□□□□□ □□□ □□ □ □□□□.
□□ □□□□□□□ "pod-reader"□□ □□□ □□ □□□ □□□.
□□: □□□□
□□□□□:
□□: □□ □□
□□□□□□: □□□
□□:
□□ □□□ "□□"□ □□□ □ □□□□.
- □□: □□□
□□: jane # "□□"□ □□□□□ □□□□□.
api□□: rbac.authorization.k8s.io
□□□□:
"roleRef"□ □□/ClusterRole□ □□ □□□□ □□□□□.
□□: □□ #□□□ □□ □□ ClusterRole□□□ □□□.
name: pod-reader # □□□ apiGroup: rbac.authorization.k8s.io apiVersion: rbac.authorization.k8s.io/v1 □□:
□□ □□□□□□ □□□□□□ □□ □□ ClusterRole□ □□□ □□□□ □□□.
□□□□□□: □□□
□□: □□ □□
□□:
- apiGroups: [""] # ""□ □□ API □□□ □□□□□.
□□□: ["□□"]
□□: ["get", "watch", "list"]

NEW QUESTION: 15
□□□□: □□□
□□□ □□: 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□ □□□□ □ □□ □ □□□ □□□□.
□□□□□□: □□
□□ □□: mysecret-pod

□□□□ □□: db-container
□□□: □□□
□□ □□: secret-vol
□□□ □□: /etc/mysecret
Answer:

NEW QUESTION: 16
□□ □□□□/□□□□ □ □□□ □□□□ □□□.
□□□□: □□
□□□ □□: □□□
□□□ □□: worker1
□□ □□□ □□□□ □□□□/□□ □□□□□ □□□ □ □□□□.
[desk@cli] $ kubectl □□ □□ □□□□ □□
□□: AppArmor□ worker1 □□□□ □□□□□□.
□:
worker1 □□□□
1. /etc/apparmor.d/nginx□ □□ □□□ AppArmor □□□□ □□□□□.
2. /home/cert_masters/nginx.yaml□ □□ □□□ □□□□□ □□□ □□□□ □□ □□□□ □□□□□.
3. □ □□□□□□ □□□□ □□□ □□□□□.
Answer:
[desk@cli] $ssh □□□1
[worker1@cli] $apparmor_parser -q /etc/apparmor.d/nginx
[worker1@cli] $aa-□□ | □□ nginx
nginx-□□□-1
[worker1@cli] $ □□□□
[desk@cli] $vim nginx-deploy.yaml
□□□□□ □□□ □□ □□ □□□□□.
□□: # □ □□ □□□□□.
container.apparmor.security.beta.kubernetes.io/<□□□□ □□>: localhost/nginx-profile-1
[desk@cli] $kubectl □□ -f nginx-deploy.yaml
□□
[desk@cli] $ssh □□□1
[worker1@cli] $apparmor_parser -q /etc/apparmor.d/nginx
[worker1@cli] $aa-□□ | □□ nginx
nginx-□□□-1
[worker1@cli] $ □□□□
[desk@cli] $vim nginx-deploy.yaml
[desk@cli] $kubectl apply -f nginx-deploy.yaml pod/nginx-deploy created □□:
https://kubernetes.io/docs/tutorials/clusters/apparmor/ pod/nginx-deploy created

[desk@cli] $kubectl apply -f nginx-deploy.yaml pod/nginx-deploy created □□:
https://kubernetes.io/docs/tutorials/clusters/apparmor/

NEW QUESTION: 17
□□ □□□ □□□□ □□□□/□□ □□□□□ □□□ □ □□□□. [desk@cli] $ kubectl config use-context dev □□□□: CIS Benchmark □□□ kubeadm □□ □□□□□ □□ □□□□□□ □□□□ □ □□ □□□ □□□□□□. □□: □□□ □□ □□ □□□ □□□□ □□□ □□ □□ □□□ □□ □□□□ □ □□□ □□ □□□ □□□. API □□□ □□ □□□ □□ □□ □□□ □□ □□□□□□. 1.2.7 □□ □□ □□□ AlwaysAllow□ □□□□ □□ FAIL 1.2.8 □□ □□ □□□ □□ □□ FAIL 1.2.7 □□ □□ □□□ RBAC FAIL □□ Kubelet□ □□ □□□ □□ □□ □□: 4.2.1 anonymous-auth □□□ false□ □□□□□□ □□□□□. FAIL 4.2.

Answer:
worker1 $ vim /var/lib/kubelet/config.yaml
□□□:
□□□□: true # □□□ □□□□□.
□□: false # □□□□ □□
□□ □□:
□□: AlwaysAllow #Delete this
□□: Webhook #□□□□ □□□
worker1 $ systemctl kubelet□ □□ □□□□□. # kubelet □□ ssh□ master1 master1□ □□ □□□□□ $ vim /etc/kubernetes/manifests/kube-apiserver.yaml - -- authorization-mode=Node,RBAC master1 $ vim /etc/kubernetes/manifests/etcd.yaml - --client -cert-auth=true □□ ssh to worker1 worker1 $ vim /var/lib/kubelet/config.yaml apiVersion: kubelet.config.k8s.io/v1beta1 □□:
□□□:
□□□□: true # □□□ □□□□□.
□□: false # □□□□ □□
□□:
□□TTL: 0□
□□□: □
x509:
clientCAFile: /etc/kubernetes/pki/ca.crt
□□ □□:
□□: AlwaysAllow #Delete this
□□: Webhook #□□□□ □□□

□□:
□□□□TTL: 0□
□□□□TTL: 0s
cgroupDriver: □□□
□□□□DNS:
- 10.96.0.10
□□□□□□□: cluster.local
cpuManagerReconcilePeriod: 0s
evictionPressureTransitionPeriod: 0□
fileCheckFrequency: 0s
healthzBind□□: 127.0.0.1
□□ □□: 10248
httpCheckFrequency: 0□
□□□□□GCAage: 0□
□□: KubeletConfiguration
□□: {}
nodeStatusReportFrequency: 0□
nodeStatusUpdateFrequency: 0□
resolvConf: /run/systemd/resolve/resolv.conf
□□□□□: true
□□□ □□ □□ □□: 0□
staticPodPath: /etc/kubernetes/manifests
streamingConnectionIdleTimeout: 0□
syncFrequency: 0s
volumeStatsAggPeriod: 0□
worker1 $ systemctl kubelet□ □□ □□□□□. # kubelet □□ ssh□ master1 master1□ □□ □□□□□ $
vim /etc/kubernetes/manifests/kube-apiserver.yaml
master1 $ vim /etc/kubernetes/manifests/etcd.yaml

NEW QUESTION: 18
□□ □□□ □□□□ □□□□/□□ □□□□□ □□□ □ □□□□.
[desk@cli] $ kubectl □□ □□ □□□□ □□
□□:
PodSecurityPolicy□ □□ □□□□□□□□ □□□ □□ Pod□ □□□ □□□□□.
□:
1. □□ □□ Pod □□□ □□□□ deny-policy□□ □ PodSecurityPolcy□ □□□□□.
2. □□ □□□ PodSecurityPolicy □□ □□□ □□□□ □ ClusterRole □□ □□ □□□ □□□ □□□□□.
3. □□ □□□□□□ □□□□ psd-denial-sa□□ □ ServiceAccount□ □□□□.
□□□□□, □□ □□□ ClusterRole deny-access-role□ □□ □□□ ServiceAccount psp-denial-sa□ □□□
□□ limits-access-bind□□ □ ClusterRoleBindind□ □□□□□.

Answer:

□□ □□ □□□□□ □□□□ □□□ psp □□□

apiVersion: rbac.authorization.k8s.io/v1

□□: ClusterRole

□□□□□:

□□: □□□ □□ □□

□□:

- apiGroups: ['□□']

□□□: ['podsecuritypolicies']

□□: ['□□□□']

□□□ □□:

- "□□ □□"

k sa psp-denial-sa -n □□ □□

apiVersion: rbac.authorization.k8s.io/v1

□□: ClusterRoleBinding

□□□□□:

□□: □□ □□□ □

□□□□:

□□: ClusterRole

□□: □□□ □□ □□

api□□: rbac.authorization.k8s.io

□□:

- □□: ServiceAccount

□□: psp-denial-sa

□□□□□□: □□

□□

master1 $ vim psp.yaml

apiVersion: □□/v1beta1

□□: PodSecurityPolicy

□□□□□:

□□: □□ □□

□□:

privileged: false # □□□ □□ □□□ □□□□ □□□□!

□□□□:

□□: RunAsAny

□□ □□:

□□: RunAsAny

runAsUser:

□□: RunAsAny

fs□□:

□□: RunAsAny
□□:
- '*'
master1 $ vim cr1.yaml
apiVersion: rbac.authorization.k8s.io/v1
□□: ClusterRole
□□□□□:
□□: □□□ □□ □□
□□:
- apiGroups: ['□□']
□□□: ['podsecuritypolicies']
□□: ['□□□□']
□□□ □□:
- "□□ □□"
master1 $ k sa □□ psp-denial-sa -n □□
master1 $ vim cb1.yaml
apiVersion: rbac.authorization.k8s.io/v1
□□: ClusterRoleBinding
□□□□□:
□□: □□ □□□ □
□□□□:
□□: ClusterRole
□□: □□□ □□ □□
api□□: rbac.authorization.k8s.io
□□:
□□ □□□ □□ □□:
- □□: ServiceAccount
□□: psp-denial-sa
□□□□□□: □□
master1 $ k □□ -f psp.yaml master1 $ k □□ -f cr1.yaml master1 $ k □□ -f cb1.yaml □□: https://kubernetes.io/docs/concepts/policy/pod-security-policy/ master1 $ k □□ -f cr1.yaml master1 $ k □□ -f cb1.yaml master1 $ k □□ -f psp.yaml master1 $ k □□ -f cr1.yaml master1 $ k □□ -f cb1.yaml □□: https://kubernetes.io/docs/concepts/policy/pod-security-policy/

NEW QUESTION: 19
□□□□□
□□□ □□ □□ □□□ □□□□ □□□ □□ □□ □□□ □□ □□□□ □ □□□ □□□□□ □□□.
API □□□ □□ □□□ □□ □□ □□□ □□ □□□□□.- a. RotateKubeletServerCertificate □□□ true□ □□□□ □□□ □□□□□□.
□. □□ □□ □□□□ PodSecurityPolicy□ □□□□ □□□ □□□□□.

□. --kubelet-certificate-authority □□□ □□□□ □□□□□□ □□□□□.
Kubelet□ □□ □□□ □□ □□ □□□ □□ □□□□□□:- a. --anonymous-auth □□□ false□ □□□□ □ □□ □□□□□□.
□. --authorization-mode □□□ Webhook□□ □□□□ □□□ □□□□□□.
ETCD□ □□ □□□ □□ □□ □□□ □□ □□□□□□.
□. --auto-tls □□□ true□ □□□□ □□□□ □□□□□□.
□. --peer-auto-tls □□□ true□ □□□□ □□□□ □□□□□.
□□: Kube-Bench □□ □□
Answer:
API □□□ □□ □□□ □□ □□ □□□ □□ □□□□□.- a. RotateKubeletServerCertificate □□□ true□ □□□□ □□□ □□□□□□.
api □□: v1
□□: □□
□□□□□:
□□ □□□□□: null
□□:
□□ □□: kubelet
□□: □□□ □□□
□□: □□□
□□□□□□: kube-system
□□:
□□□□:
- □□:
- kube-□□□□-□□□
+ - --feature-gates=RotateKubeletServerCertificate=true
□□□: gcr.io/google_containers/kubelet-amd64:v1.6.0
livenessProbe:
□□ □□□: 8
httpGet:
□□□: 127.0.0.1
□□: /healthz
□□: 6443
□□: HTTPS
initialDelaySeconds: 15
timeoutSeconds: 15
□□: □□□
□□:
□□:
CPU: 250m
□□ □□□:

- □□□ □□: /etc/kubernetes/
□□: k8s
□□ □□: □
- □□□ □□: /etc/ssl/certs
□□: □□□
- □□□ □□: /etc/pki
□□: pki
□□□ □□□□: □
□□:
- □□□ □□:
□□: /etc/kubernetes
□□: k8s
- □□□ □□:
□□: /etc/ssl/certs
□□: □□□
- □□□ □□:
□□: /etc/pki
□□: pki
□. □□ □□ □□□□ PodSecurityPolicy□ □□□□ □□□ □□□□□.
□□: "/bin/ps -ef | grep $apiserverbin | grep -v grep"
□□□:
□□□ □□:
- □□□: "--enable-admission-plugins"
□□□□:
□□: □□
□: "PodSecurityPolicy"
□□: □
□□: |
□□□□ □□□ □□□ □□ □□ □□ □□ □□□ □□□□□.
□□ □□ API □□ □□ □□ □□ $apiserverconf□ □□□□□.
□□□ □□□□ --enable-admission-plugins □□□□□ PodSecurityPolicy□ □□□□ □□□ □□□□□.
--enable-admission-plugins=...,PodSecurityPolicy,...
□□ □□ API □□□ □□ □□□□□□.
□□: □
□. --kubelet-certificate-authority □□□ □□□□ □□□□□□ □□□□□.
□□: "/bin/ps -ef | grep $apiserverbin | grep -v grep"
□□□:
□□□ □□:
- □□□: "--kubelet-certificate-authority"
□□: □

□□: |
Kubernetes □□□□ □□□ apiserver□ kubelet □□ TLS □□□ □□□□□. □□ □□ API □□ □□ □□ □□□ □□□□□.
$apiserverconf□ □□□ □□□ □□□□ --kubelet-certificate-authority □□□□□ □□ □□□ □□□ □□ □□□ □□□□□.
--kubelet-certificate-authority=<ca-□□□>
□□: □
ETCD□ □□ □□□ □□ □□ □□□ □□ □□□□□□.
□. --auto-tls □□□ true□ □□□□ □□□□ □□□□□□.
□□□ □□□□ etcd □□ □□ □□ $etcdconf□ □□□□ --auto-tls □□□□□ □□□□□ false□ □□□□ □. --auto-tls=false b. --peer-auto-tls □□□ true□ □□□□ □□□□ □□□□□. □□□ □□□□ etcd □□ □□ □□ $etcdconf□ □□□□ --peer-auto-tls □□□□□ □□□□□ false□ □□□□□. --□□-□□-t l s□ □

NEW QUESTION: 20
□□□□: □□□□: gvisor □□□ □□: master1 □□□ □□: worker1
□□ □□□ □□□□ □□□□/□□ □□□□□ □□□ □ □□□□.
[desk@cli] $ kubectl □□ □□ □□□□ gvisor
□□□□: □ □□□□□ □□□ □□□, runc □ □□ □□□□ □□□□□ □□□□□□□.
□□: □□□ □□□ □□□ □□ runc□ □□□□ not-trusted□□ RuntimeClass□ □□□□. newruntime□□ □□□□□ □□□□□□ □□□ □□ Pod□ □□□□□□□.
Answer:
□□
[desk@cli] $vim runtime.yaml
apiVersion: node.k8s.io/v1
□□: RuntimeClass
□□□□□:
□□: □□□ □ □□
□□□: runc
[desk@cli] $k □□ -f runtime.yaml [desk@cli] $k □□ □□□□
□□ □□ □□ □□□ □□
nginx-6798fc88e8-chp6r 1/1 □□ □ 0 11□
nginx-6798fc88e8-fs53n 1/1 □□ □ 0 11□
nginx-6798fc88e8-ndved 1/1 □□ □ 0 11□
[desk@cli] $ k □□□□
□□ □□ □□ □□ □□ □□
nginx 3/3 11 3 5m
[desk@cli] $ k □□ □□ nginx

NEW QUESTION: 21

□□□□ □□□ □□□□ □□□□□ □□□□□.
□□□□□ □□□□ □□□ □□ □□
/etc/kubernetes/confcontrol □ HTTPS □□□ □□ □□□ □□□□ □□□ □□□ https://test-server.local.8081/image_policy
1. □□ □□□□□ □□□□□□.
2. □□ □□□ □□□□ □□□□ □□□ □□□ □□□□□.
□□□□□ □□□ □□□ □□□ □□□ □□□□ □□□ □□□□□□.
Answer:
ssh-□□ ~/.ssh/tempprivate
□□ "$(ssh-agent -s)"
cd □□/terraform/aws
vi terraform.tfvars
□□□□ □□□
terraform □□ -var-file=credentials.tfvars
ansible-playbook -i ./inventory/hosts ./cluster.yml -e ansible_ssh_user=core -e bootstrap_os=coreos -b --become-user=root --flush-cache -e ansible_user=core

NEW QUESTION: 22
□□□□□
□□□□□□ □□□□□ □□□ □□□ □□□□□□□ □□ □□ □□□ □□ 80□ □□□ □ □□□ □□□ □ allow-np□□ □□□□ □□□ □□□□.
□□□□ □□□ □□□□ □□□□□□.
1. □□ 80□□ □□ □□□□ □□ Pod□ □□ □□□□ □□□□ □□□□.
2. □□□□□□ □□□□□ □□ □□□□ □□□□ □□□□ □□□□.
Answer:
apiVersion: networking.k8s.io/v1
□□: NetworkPolicy
□□□□□:
□□: □□□□ □□
□□:
podSelector: {} # □□□ □□□□□□□ □□ □□□ □□□□□.
□□ □□:
- □□□□
□□:
- □□: #in □□ □□□□ 80□□□□ □□
- □□□□: TCP
□□: 80

NEW QUESTION: 23
□□□□□

□□□□□□ □□ □□□ □□□□□□ □□ □□□□ □□□□□ □□□ □□□□□□.
1. □□□ /var/log/kubernetes/kubernetes-logs.txt□ □□□□□.
2. □□ □□□ 5□□ □□□□□.
3. □□ 10□□ □□ □□ □□ □□□ □□□□□.
□□□ □□□ □□ □□□ □□□□ □□□□□.
1. RequestResponse□□ Cronjobs □□
2. □□□□□□ kube-system□□ □□ □□ □□□ □□ □□□ □□□□□.
3. □□ □□□□ □□ □ □□□ □□ □□ □□□□ □□□□□.
4. □□□□□□□ "system:kube-proxy"□ □□ □□ □□□ □□□□ □□□□.
A. □□□□ □□□□□□.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 24
□□□□ □□□ □□□ □□ 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- □□□ tcp 0 0 :::443 :::* LISTEN 9571/docker-proxy 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 State Recv-Q Send-Q □□ □□:□□ □□ □□:□□
tcp LISTEN 0 128 0.0.0.0:22 0.0.0.0:* □□□:("sshd",pid=575,fd=3))

NEW QUESTION: 25
□□
AppArmor□ □□□□□ □□□ □□□□ □□□□□□. AppArmor □□□□ □□□□□□ □□ □□□□ □ □□□□.
□
□□□□□ □□□ □□□□ /etc/apparmor.d/nginx_apparmor□ □□ □□□ AppArmor □□□□ □□□□□.
/home/candidate/KSSH00401/nginx-pod.yaml□ □□ □□□ □□□□□ □□□ □□□□ AppArmor □□□□ □□□□□.
□□□□□ □□□□□ □□□ □□□□ □□□ □□□ Pod□ □□□□.

Answer:

NEW QUESTION: 26
□□□□□□ □□□ □□ □□ □□ Nginx-pod□ □□□□ □□□ □□□□□ □□□□ nginx-svc□□ Nginx-□□ □□ □□□□ □□□□ □□ □□□ tls□□ □□□□□ □□□□□.
A. □□ □□ □□□□ □□□□□□.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 27
□□□□□
□. □□□ □□□□□□□□ default-token-xxxxx□□ □□ □□□ □□□□ □□□□□.
□□ □□ token.txt□ □□
□. □□ □□□□ □□□□ DB □□□□□□□ test-db-secret□□□ □ □□□ □□□□□.
□□□ □□: mysql
□□□□: password@123
/etc/mysql-credentials □□□ □□□ □□ test-db-secret□ □□□□ □ □□ □□□□□□ db□ □□□ nginx □ □□ □□ 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 □□□□ □□ | grep -E '□□□□□ □□□|□□□□□ □□□ □□□' | awk '/http/ {print $NF}' CA □□ □(□□) - □□□□□ □□□□□ □□□ Kubernetes □□□□ □□□□□. □□□□□ □□□ □□□□ □□ □□□.
kubectl get secrets□ □□□□ □□□ □□□□ default-token-xxxxx□ □□□ □□□ □□□□ □□□. □□□ □ □□□□ □□ □□ □□ □□□ □□□□□□.
□□ □□□ □□□□ □□□□ □□□□□.
kubectl get secret <□□ □□> -o jsonpath="{['data']['ca\.crt']}"

NEW QUESTION: 28

□□□□□□ test-system□□ □□ □□ nginx-pod□□ □□ □□□ □□□ □□□ service-account-name□ □□□□ /candidate/KSC00124.txt□ □□□□ □□□□. □□□□□□ test-□□ dev-test-role□□□ □ □□ □ □□□□. □□□□□□ □□□ □□□□ □□ □□□□ □□□ □□□ □ □□ □□□□□□.
□□ □□□ Role□ □□□ ServiceAccount(□□□□□□ test-system□□ □□ □□ Nginx □□□ □□)□ □ □□□□ dev-test-role-binding□□□ □ RoleBinding□ □□□□□.
Answer:

NEW QUESTION: 29
□□□□□
□□□□□□ □□□ □□ □□ □□ Nginx-pod□ □□□□ □□□ □□□□□ □□□□ nginx-svc□□ Nginx-□□ □□ □□□□ □□□□ □□ □□□ tls□□ □□□□□ □□□□□.
A. □□□□ □□□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 30
□□ □□□ □□□□ □□□□/□□ □□□□□ □□□ □ □□□□.
[desk@cli] $ kubectl □□ □□ □□□□ □□□ □□
□□: □□□□□□ □□ □□□ □□□□□□.
□□□ □□□ □□ □□□□ □□□□□ □□□ □□□□□□.
1. □□□ /var/log/Kubernetes/logs.txt□ □□□□□.
2. □□ □□□ 5□ □□ □□□□□.
3. □□ 10□□ □□ □□ □□ □□□ □□□□□.
□□ □□□ /etc/Kubernetes/logpolicy/audit-policy.yaml□□ □□□□□. □□□□ □□ □□□ □□□□□.
□□: □□ □□□ □□□□□ □□□ □□□ □□□□.
□□□ □□□ □□ □□□ □□□□ □□□□□.
1. RequestResponse □□□□ □□ □□
2. □□□□□□ □□□□□□□ □□ □□□ □□ □□ □□
3. □□□□□ □□□□ □□ □□□□□□□ ConfigMap □ □□ □□ □□ □□□□□ □□□□ □□ □□ □ □□ □□□□ □□ □□□ □□□□□. □□: □□□ □□□ □□□□ □□ □□ □□□□.
Answer:
$ vim /etc/kubernetes/log-policy/audit-policy.yaml
- □□: □□ □□
□□□ □□: ["□□□:□□"]
- □□: □□
□□:
- □□: "" # □□ API □□
□□□: ["□□ □□"]
□□□□□□: ["□□□□□"]
- □□: □□□□□
□□:

- □□: ""
□□□: ["configmaps", "□□"]
- □□: □□□□□
$ vim /etc/kubernetes/manifests/kube-apiserver.yaml
□□
- --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
□□
[desk@cli] $ SSH □□□1
[master1@cli] $ vim /etc/kubernetes/log-policy/audit-policy.yaml
apiVersion: audit.k8s.io/v1 # □□ □□□□□.
□□: □□
RequestReceived □□□ □□ □□□ □□ □□ □□□□ □□□□ □□□□.
□□ □□:
- "□□ □□□"
□□:
□□□□□ □□ □□□□□ "system:kube-proxy"□ □□ □□ □□□ □□□□ □□□□.
- □□: □□
□□□: ["□□□:kube-proxy"]
□□: ["□□"]
□□:
- □□: "" # □□ API □□
□□□: ["□□□□□", "□□□"]
□□ □□□ URL □□□ □□ □□□ □□□ □□□□ □□□□.
- □□: □□
□□□ □□: ["□□□:□□□"]
nonResourceURL:
- "/api*" # □□□□□ □□.
- "/□□"
□□□ □□ □□□ □□□□□□
- □□: □□ □□
userGroups: ["system:nodes"] # □□ □□
- □□: □□
□□:
- □□: "" # □□ API □□
resources: ["persistentvolumes"] # □□ □□ □□
namespaces: ["frontend"] # □□□□□ ns□ □□ □□ □□
- □□: □□□□□

□□:
- □□: "" # □□ API □□
resources: ["configmaps", "secrets"] # configmaps & secrets □□
- level: Metadata # □□ □□ □□ □□ □□
[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
□□:
□□□□:
- □□:
- kube-apiserver
- --advertise-address=10.0.0.5
- --allow-privileged=true
- --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/ □□: □ □ □□ □ □□ □□□ □□ vim /etc/kubernetes/manifests/kube-apiserver.yaml□ □□□□□ □□□□ □□ □ □□□ □□□□. □□□□□□□. □□: https://kubernetes.io/docs/tasks/debug-application-cluster/audit/

NEW QUESTION: 31
□□
CIS Benchmark □□□ kubeadm□ □□□ □□□□□ □□ □□□□□□ □□ □□□□ □□ □□ □□□ □ □□□□□.
□
□□□ □□ □□ □□□ □□□□ □□□ □□ □□ □□□ □□ □□□□ □ □□□ □□□□□ □□□.
API □□□□ □□□ □□ □□ □□□ □□ □□□□□.
Kubelet□□ □□□ □□ □□ □□□ □□ □□□□□.

etcd□ □□ □□□ □□ □□ □□□ □□ □□□□□.
Answer:

NEW QUESTION: 32
□□□ □□□□□□□ □□ □□□□ □□ □□ □□□ □□□□ PSP□ □□□□.
□□□ □□ □□□ □□ □□ □□□ □□□ □□□□□ □□ □□□□ prevent-volume-policy□□ □ PodSecurityPolicy□ □□□□.
□□□ □□□□□□□ psp-sa□□ □ ServiceAccount□ □□□□.
□□ □□□ □□ □□ □□ prevent-volume-policy□ □□□□ psp-role□□□ □ ClusterRole□ □□□□□.
□□□ ClusterRole psp-role□ □□□ SA psp-sa□ □□□□□ psp-role-binding□□□ □ ClusterRoleBinding □ □□□□□.
□□:
□□ □□□ □□□□□ □□□□□ □□ □□□□□□□ □□ □□□□ □□□□ □□□□ □□□.
POD □□□□□:
api □□: v1
□□: □□
□□□□□:
□□:
□□:
□□□□:
- □□:
□□:
□□ □□□:
- □□:
□□□ □□:
□□:
- □□:
□□:
□□ □□:
Answer:
apiVersion: □□/v1beta1
□□: PodSecurityPolicy
□□□□□:

□□: □□□
□□:
seccomp.security.alpha.kubernetes.io/allowedProfileNames: 'docker/default,runtime/default'
apparmor.security.beta.kubernetes.io/allowedProfileNames: 'runtime/default'
seccomp.security.alpha.kubernetes.io/defaultProfileName: '□□□/□□'
apparmor.security.beta.kubernetes.io/defaultProfileName: '□□□/□□' □□:
□□: □□
□□□□ □□□□□□□ □□□□ □□ □□□□□.
allowPrivilegeEscalation: □□
□□□ □□□ □□ + □□ □□□□□□□ □□□□ □□ □□ □□□□□.
□□□ □□ □□□ □□ □□□ □ □□□□.
requiredDropCapabilities:
- □□
□□ □□ □□□ □□□□□.
□□:
- 'configMap'
- 'emptyDir'
- '□□'
- '□□'
- '□□ API'
□□□□ □□□□ □□□ □□□□□□□□ □□□□□ □□□□□ □□□□□.
- 'persistentVolumeClaim'
□□□ □□□□: □□
hostIPC: □□
hostPID: □□
runAsUser:
□□□□□ □□ □□ □□ □□□□□ □□□□□.
□□: 'MustRunAsNonRoot'
□□□□:
□ □□□ □□□ SELinux□ □□ AppArmor□ □□□□□ □□□□□.
□□: 'RunAsAny'
□□ □□:
□□: 'MustRunAs'
□□:
□□ □□ □□ □□.
- □□: 1
□□: 65535
fs□□:
□□: 'MustRunAs'
□□:

□□ □□ □□ □□.
- □□: 1
□□: 65535
□□ □□ □□ □□ □□□: □□

NEW QUESTION: 33
□□
□□□□ □□□ □□□□ □□□□□ □□□□□□ □□ □□□□ □□□ □□□ □□□□ □□□□□. □□ □□ □□□□ □□□ □□□□ □□□ □□□□ □□□□ □□□ □□□□□.
□
/etc/kubernetes/epconfig □□□□□ □□□□ □□□ HTTPS □□□□□
https://wakanda.local:8081 /image_policy□ □□ □□□□ □□□□ □□□ □□□□ □□ □□:
1. □□□ □□ □□□ □□□ □□□□ □□□
2. □□ □□□ □□□□ □□□ □□□ □□
3. □□□ HTTPS □□□ □□□□ □□□□□ □□□ □□□□□. □□□□□ □□□ □□□
□ /root/KSSC00202/vulnerable-resource.yml□ □□□□ □□□ □□□□□ □□□□□□.
Answer:

NEW QUESTION: 34
□□□□: □□ □□□□
□□□ □□: □□□
□□□ □□: worker1
□□ □□□ □□□□ □□□□/□□ □□□□□ □□□ □ □□□□.
[desk@cli] $ kubectl □□ □□ □□□□ □□ □□□□
□□:
□□□□ □□□ □□□□ □□□□□ □□□□□□ □□ □□□□ □□□ □□□ □□□□ □□□□□. □□ □□ □□□□ □□□ □□□□ □□□ □□□□ □□□□ □□□ □□□□□.
□:
□□ □□□□ □□□ □□□□ □□□ □□□□□ □□□ □□□□ □□ □□□ □□□□ □□□.
/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:
[master@cli] $ cd /etc/Kubernetes/config
1. □□□□□ □□□□□ kubeconfig □□
[master@cli] $ vim kubeconfig.json

"defaultAllow": false # □□□□ □□
2. ~/.kube/config□□ □□ □□ □□□ □□ □□□□□ □□□□□.
[master@cli] $cat /etc/kubernetes/config/kubeconfig.yaml | grep □□
□□□ □□:
3. ImagePolicyWebhook □□□
[master@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 □□□
[master@cli] $ cd /etc/Kubernetes/config
[master@cli] $ vim kubeconfig.json
{
"□□□ □□": {
"kubeConfigFile": "/etc/kubernetes/config/kubeconfig.yaml",
"allowTTL": 50,
"□□TTL": 50,
"□□□□□□": 500,
"defaultAllow": true # □□
"defaultAllow": false # □□
}
}
□□: □□□□ □□□ □□ □ □ □□□□ □ □□ □□□ □□□ □ □□□□?
[master@cli] $cat ~/.kube/config | grep □□
□□
[master@cli] $cat /etc/kubernetes/manifests/kube-apiserver.yaml
[master@cli] $vim /etc/kubernetes/config/kubeconfig.yaml
[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: 35

kubesec □□ □□□□ □□□□ □□□ YAML □□□□□□ □□□□ □□ □□ □□□ □□ □ □□□□ 4 □ □□□□ □□□□□□.

kubesec-test.yaml

api □□: v1

□□: □□

□□□□□:

□□: kubesec-□□

□□:

□□□□:

- □□: kubesec-demo

□□□: gcr.io/google-samples/node-hello:1.0

□□ □□□□:

readOnlyRootFilesystem: □

□□: docker run -i kubesec/kubesec:512c5e0 scan /dev/stdin < kubesec-test.yaml

Answer:

kubesec □□ k8s-deployment.yaml

□□□ <<EOF> kubesec-test.yaml

api □□: v1

□□: □□

□□□□□:

□□: kubesec-□□

□□:

□□□□:

- □□: kubesec-demo

□□□: gcr.io/google-samples/node-hello:1.0

□□ □□□□:

readOnlyRootFilesystem: □

EOF

kubesec □□ kubesec-test.yaml

docker run -i kubesec/kubesec:512c5e0 scan /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":"HTTP □□ □□ □□ 8080"} curl -sSX POST --data-binary @test/asset/score-0-cap-sys-admin.yml http://localhost:8080/scan

[

{

"□□": "□□/□□ □□□□-demo.default",

"□□": □,

"message": "-30□□□ □□",

"□□": -30,

"□□": {
"□□□□": [
{
"□□□": "□□□□[] .securityContext .capabilities .add == SYS_ADMIN",
"reason": "CAP_SYS_ADMIN□ □□ □□□ □□ □□□□ □□ □□□ □□□."
},
{
"□□□": "□□□□[] .securityContext .runAsNonRoot == □",
"□□": "□□ □□□ □□□□ □□ □□ □□ □□□□ □□□ □□ □□□□ □□ □□"
},
// ...

NEW QUESTION: 36
□. □□□ □□□□□□□□ default-token-xxxxx□□ □□ □□□ □□□□ □□□□□.
□□ □□ token.txt□ □□
□. □□ □□□□ □□□□ DB □□□□□□□ test-db-secret□□□ □ □□□ □□□□□.
□□□ □□: mysql
□□□□: password@123
/etc/mysql-credentials □□□ □□□ □□ test-db-secret□ □□□□ □ □□ □□□□□□ db□ □□□ nginx □ □□ □□ 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 □□□□ □□ | grep -E '□□□□□ □□□|□□□□□ □□□ □□□' | awk '/http/ {print $NF}' CA □□ □(□□) - □□□□□ □□□□□ □□□ Kubernetes □□□□ □□□□□. □□□□□ □□□ □□□□ □□ □□□.
kubectl get secrets□ □□□□ □□□ □□□□ default-token-xxxxx□ □□□ □□□ □□□□ □□□. □□□ □ □□□□ □□ □□ □□ □□□ □□□□□□.
□□ □□□ □□□□ □□□□ □□□□□.

kubectl get secret <□□ □□> -o jsonpath="{['data']['ca\.crt']}"

NEW QUESTION: 37
□□□□□
□□□ Dockerfile □□ □ □□
□□□□□: □□
□□ apt-get □□□□ -y
□□ apt-install nginx -y
entrypoint.sh □□ /
□□□□□□ ["/entrypoint.sh"]
□□□ □□
□□□ □□ □□ □□ □□□ □□□ □□ □ □□ □□□ □□□□□. □□ □□□□□ □□ apiVersion: v1 □
□: Pod □□□□□□ □□□□ □□□□□.
□□: security-context-demo-2
□□:
□□ □□□□:
runAsUser: 1000
□□□□:
- □□: sec-ctx-demo-2
□□□: gcr.io/google-samples/node-hello:1.0
□□ □□□□:
runAsUser: 0
□□: □
allowPrivilegeEscalation: □□
□□□ □□ □□ □□ □□□ □□□ □□ □ □□ □□□ □□□□□. □□ □□□ □□□□□ □□□□ □□
□□. □□ □□ □□□ □□ □□□ □□ □□□ □□ □□□□ □□□ □□□ □□□ ID 5487□ □□ □□□
test-user□ □□□□□□.
A. □□□□ □□□□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 38
□□□ □□ □□ Falco□ □□□□ □□ □□□□ □□□□ □□□□□ □□□□ □□□ □□□□ □□ 30□
□□ □□□□ □□□ □□□□□.
A. □□□ □□□ □□□ □□ □□ art /opt/falco-incident.txt□ □□□□□. □□□□ □ □□ □□□
Answer: A (LEAVE A REPLY)
[□□□□□],[uid],[□□□ □□],[□□□□ □□]

NEW QUESTION: 39
□□□□□

□□□□□□ test-system□□ □□ □□ nginx-pod□□ □□ □□□ □□□ □□□ service-account-name□ □□□□ /candidate/KSC00124.txt□ □□□□ □□□□. □□□□□□ test-□□ dev-test-role□□□ □ □□ □ □□□□. □□□□□□ □□□ □□□□ □□ □□□□ □□□ □□□ □ □□ □□□□□□.
□□ □□□ Role□ □□□ ServiceAccount(□□□□□□ test-system□□ □□ □□ Nginx □□□ □□)□ □ □□□□ dev-test-role-binding□□□ □ RoleBinding□ □□□□□.

A. □□□□ □□□□□.

Answer: (SHOW ANSWER)