Quiz CKS - High Pass-Rate Certified Kubernetes Security Specialist (CKS) Latest Test Practice

DOWNLOAD the newest Itcertmaster CKS PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1FsFu069mvgSqw4NMR1fSNsOAt0LIiPan

Many students often feel that their own gains are not directly proportional to efforts in their process of learning. This is because they have not found the correct method of learning so that they often have low learning efficiency. If you have a similar situation, we suggest you try CKS practice materials. CKS test guide is compiled by experts of several industries tailored to CKS Exam to help students improve their learning efficiency and pass the exam in the shortest time. CKS test guide involve hundreds of professional qualification examinations. No matter which industry you are in, CKS practice materials can meet you.

The Linux Foundation CKS Exam is a proctored, online exam that lasts for two hours. It comprises 17-20 performance-based tasks of various complexities that test candidates' knowledge, skills, and ability to secure Kubernetes environments. CKS exam covers several topics that include, but are not limited to, cluster setup, container images, networking, runtime environments, policy and access control, auditing and logging, and supply chain security. The tasks are designed to challenge candidates on different aspects of Kubernetes security, including how to configure Docker image vulnerabilities, secure cluster networking, and hardening Kubernetes nodes among many other topics.

>> CKS Latest Test Practice <<

Free PDF Quiz 2026 CKS: Valid Certified Kubernetes Security Specialist (CKS) Latest Test Practice

The online version of CKS quiz torrent is based on web browser usage design and can be used by any browser device. The first time you use CKS test preps on the Internet, you can use it offline next time. CKS learn torrent does not need to be used in a Wi-Fi environment, and it will not consume your traffic costs. You can practice with CKS Quiz torrent at anytime, anywhere. On the other hand, the online version has a timed and simulated exam function.

Linux Foundation Certified Kubernetes Security Specialist (CKS) Sample Questions (Q54-Q59):

NEW QUESTION # 54
SIMULATION
Documentation Deployments, Pods, Falco
You must connect to the correct host . Failure to do so may result in a zero score.
[candidate@base] $ ssh cks000026
Context
A Pod is misbehaving and poses a security threat to the system.
Task
One of the Pods belonging to the application ollama is misbehaving. It is directly accessing the system's memory reading from the sensitive file /dev/mem.
First, identify the misbehaving Pod accessing /dev/mem.

The cluster uses the Docker Engine as its container runtime . If needed, use the docker command to troubleshoot running containers.
Next, identify the Deployment managing the misbehaving Pod and scale it to zero replicas.
Do not modify the Deployment except for scaling it down.
Do not modify any other Deployments .
Do not delete any Deployments.

Answer:

Explanation:
See the Explanation below for complete solution
Explanation:
1) Connect to the correct host
ssh cks000026
sudo -i
2) Identify the misbehaving Pod accessing /dev/mem
This task hints Falco is available → use it first (fast + intended).
2.1 Check Falco logs for /dev/mem access
journalctl -u falco | grep dev/mem
If Falco runs as a pod instead of systemd:
kubectl -n falco logs -l app=falco | grep dev/mem
2.2 Identify the Pod name
From the Falco output, you will see something like:
Pod=ollama-xxxxx Namespace=default File=/dev/mem
Note the exact Pod name (example: ollama-7c9d6f7b6d-abcde)
3) (If Falco logs are unclear) Confirm using Docker runtime
Because the cluster uses Docker, verify which container is accessing /dev/mem.
3.1 List running containers
docker ps
3.2 Inspect suspicious container
(Find container related to ollama)
docker inspect <container_id> | grep ollama
You should confirm it maps to the same Pod you saw in Falco.
4) Identify the Deployment managing the misbehaving Pod
4.1 Get Pod details
kubectl get pod <MISBEHAVING_POD_NAME> -o wide
4.2 Find owning Deployment
kubectl get pod <MISBEHAVING_POD_NAME> -o jsonpath='{.metadata.ownerReference[0].name}' This will output something like:
ollama
That is the Deployment name
5) Scale ONLY that Deployment to zero replicas
Do not edit, delete, or touch anything else
kubectl scale deployment ollama --replicas=0
6) Verify the Pod is terminated
kubectl get pods | grep ollama
Expected: no running Pods
Also confirm replicas:
kubectl get deployment ollama
Replicas should show:
0/0

NEW QUESTION # 55
You are running a web application in a Kubernetes cluster using a Deployment. You want to implement a security measure to ensure that the application container only has access to the necessary system calls and files. You're worried about potential exploits that could give the container excessive privileges. Explain how you would use Seccomp profiles to achieve this, and provide an example Seccomp profile using a JSON format.

Answer:

Explanation:

Solution (Step by Step) :
1. Understand Seccomp: Seccomp (Secure Computing Mode) is a Linux kernel feature that allows you to restrict the system calls that a process can make. You can define a profile that lists the allowed system calls, effectively creating a "sandbox" for the container.
2. Create a Seccomp Profile: You can create a Seccomp profile in a JSON format. Here's an example:
3. Apply the Seccomp Profile: You can apply the Seccomp profile to your container using the 'securitycontext' field in your Deployment YAML.
4. Test and Verify: After deploying your Deployment, test your application and make sure it functions as expected. You can verity that the Seccomp profile is working by attempting to run commands within the container that are not allowed by your profile.

NEW QUESTION # 56
SIMULATION
Create a RuntimeClass named gvisor-rc using the prepared runtime handler named runsc.
Create a Pods of image Nginx in the Namespace server to run on the gVisor runtime class

Answer:

Explanation:
SeetheExplanationbelowExplanation:
Install the Runtime Class for gVisor
{ # Step 1: Install a RuntimeClass
cat <<EOF | kubectl apply -f -
apiVersion: node.k8s.io/v1beta1
kind: RuntimeClass
metadata:
name: gvisor
handler: runsc
EOF
}
Create a Pod with the gVisor Runtime Class
{ # Step 2: Create a pod
cat <<EOF | kubectl apply -f -
apiVersion: v1
kind: Pod
metadata:
name: nginx-gvisor
spec:
runtimeClassName: gvisor
containers:
- name: nginx
image: nginx
EOF
}
Verify that the Pod is running
{ # Step 3: Get the pod
kubectl get pod nginx-gvisor -o wide
}

NEW QUESTION # 57
use the Trivy to scan the following images,
1. amazonlinux:1
2. k8s.gcr.io/kube-controller-manager:v1.18.6
Look for images with HIGH or CRITICAL severity vulnerabilities and store the output of the same in /opt/trivy-vulnerable.txt

- A. Send us your suggestion
- B. Send us your suggestion on it.

Answer: B

NEW QUESTION # 58
You are running a critical application in your Kubernetes cluster and want to minimize the attack surface by removing unnecessary features from the cluster- You need to identify and disable features that are not essential for your application.

Answer:

Explanation:
Solution (Step by Step):
1. Review Cluster Features: Analyze your cluster configuration and identity features that are not used by your critical application. This might include unnecessary network services, ingress controllers, or resource quotas.
2. Disable Unused Features:
- Network Services: You might disable or remove network services that are not required for your application's functionality. This could include removing unused NodePons or disabling unused Ingress controllers.
- Ingress Controllers: If you are not using Ingress controllers, disable them or remove the associated configuration.
- Resource Quotas: If you do not need resource quotas for your application, disable them.
- Other Features: You can disable other features like the dashboard, network policy enforcement, or other security features that you may not require.
3. Disable Unnecessary Components: Remove unused components or services that are not essential for your application.
4. Minimize Services Exposed to the Internet: Only expose the necessary services to the public internet and restrict access to other services to authorized users or applications.

NEW QUESTION # 59
.....

The Certified Kubernetes Security Specialist (CKS) (CKS) practice questions are designed by experienced and qualified CKS exam trainers. They have the expertise, knowledge, and experience to design and maintain the top standard of Certified Kubernetes Security Specialist (CKS) (CKS) exam dumps. So rest assured that with the Certified Kubernetes Security Specialist (CKS) (CKS) exam real questions you can not only ace your Certified Kubernetes Security Specialist (CKS) (CKS) exam dumps preparation but also get deep insight knowledge about Linux Foundation CKS exam topics. So download Certified Kubernetes Security Specialist (CKS) (CKS) exam questions now and start this journey.

lms.uplyx.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, courses.beinspired.co.za, www.stes.tyc.edu.tw, elearning.pumwanicollege.ac.ke, Disposable vapes

P.S. Free & New CKS dumps are available on Google Drive shared by Itcertmaster: https://drive.google.com/open?id=1FsFu069mvgSqw4NMR1fSNsOAt0LIiPan