# CKS New Dumps & Latest CKS Exam Online

What's more, part of that PDFBraindumps CKS dumps now are free: https://drive.google.com/open?id=1FOhQMk8diXcS-PX2S1NT4y-hOH5RB3tA

CKS certifications are thought to be the best way to get good jobs in the high-demanding market. There is a large range of CKS certifications that can help you improve your professional worth and make your dreams come true. Our CKS Certification Practice materials provide you with a wonderful opportunity to get your dream certification with confidence and ensure your success by your first attempt.

The CKS certification exam is a rigorous assessment of the candidate's skills, covering a wide range of important topics such as hardening cluster components, securing network connectivity, and ensuring secure access to Kubernetes API and etcd. CKS Exam consists of 15-20 performance-based tasks and scenarios that test the candidates' hands-on skills in securing a Kubernetes cluster. CKS exam is three hours long and is proctored online.

**>> CKS New Dumps <<**

## CKS New Dumps – Latest updated Latest Exam Online Provider for CKS: Certified Kubernetes Security Specialist (CKS)

With vast experience in this field, PDFBraindumps always comes forward to provide its valued customers with authentic, actual, and genuine CKS exam dumps at an affordable cost. All the CKS questions given in the product are based on actual examination topics. PDFBraindumps regularly updates CKS Practice Exam material to ensure that it keeps in line with the test. In the same way, PDFBraindumps provides a free demo before you purchase so that you may know the quality of the CKS dumps.

## Linux Foundation Certified Kubernetes Security Specialist (CKS) Sample Questions (Q48-Q53):

**NEW QUESTION # 48**
You are using Kubesec for static analysis of Kubernetes manifests. You have a Deployment YAML file containing a container image that pulls from a public registry. The analysis reveals a potential vulnerability: the container image is outdated. How would you use Kubesec to identify this vulnerability and what steps would you take to remediate it?

**Answer:**

Explanation:
Solution (Step by Step) :
1. Run Kubesec Analysis:
- Use the 'kubesec' command to analyze your Deployment YAML file:

bash

kubesec scan your-deploymentyaml

- Kubesec will provide a detailed report of potential security vulnerabilities and best practice recommendations.

2. Identify Outdated Image:

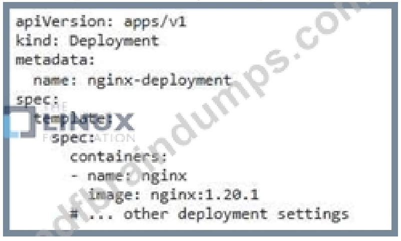
- Review the Kubesec report to identify the warning related to the outdated container image. Kubesec might provide specific information like the image
name, tag, and the reason it's considered outdated (e.g., known vulnerabilities, end-of-life support).

3. Check for Updates:

- Check the official repository or documentation of the container image for newer versions.
- Look for updated tags that address the identified vulnerability or have updated security patches.

4. Update Deployment YAML:

- Modify your Deployment YAML file to use the newer, updated container image.
- Example (assuming the updated image is 'nginx:1 .20.1'):



```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: nginx-deployment
spec:
  template:
    spec:
      containers:
      - name: nginx
        image: nginx:1.20.1
      # ... other deployment settings
```

5. Re-run Kubesec Analysis: - After updating the Deployment YAML, run Kubesec analysis again. This will verify that the vulnerability is resolved and that the new container image is properly configured.

**NEW QUESTION # 49**

You are running a Kubernetes cluster with a deployment named "my-app" that uses a container image from a public registry. You suspect that a recent deployment update may have introduced a vulnerability in one of the containers. Describe how you can use container image scanning tools like Trivy to identify and address the vulnerability.

**Answer:**

Explanation:

Solution (Step by Step) :

1. Install and Configure Trivy:

- Install Trivy on your system or Within your Kubernetes cluster. Trivy is a versatile vulnerability scanner that can scan container images, filesystems, and applications.

2. Scan the Container Image:

- Run Trivy against the container image used by the "my-app" deployment.

bash

trivy image example/nginx:latest

3. Analyze the Scan Results:

- Review the Trivy scan report, which will list any vulnerabilities detected in the container image. The report will provide information like the vulnerability's severity, description, and potential impact.

4. Address the Vulnerability:

- If vulnerabilities are discovered, take appropriate actions to mitigate the risk. This could involve:
- Updating the Container Image: If a newer version of the container image is available with the vulnerability patched, update the deployment to use the updated image.
- Implementing Security Measures: Consider implementing additional security controls within your containers, such as restricting network access, limiting container privileges, or using security-enhancing tools.
- Accepting the Risk: If the vulnerability is deemed low risk and updating or mitigating it is not feasible, you may choose to accept the risk and monitor the vulnerability closely.

5. Integrate with CI/CD Pipeline:

- Integrate Trivy into your CI/CD pipeline to automatically scan container images before they are deployed to your Kubernetes cluster. This helps to catch vulnerabilities early and prevents them from being introduced into your production environment.

**NEW QUESTION # 50**

Cluster: qa-cluster

Master node: master Worker node: worker1

You can switch the cluster/configuration context using the following command:

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

Task:
Create a NetworkPolicy named restricted-policy to restrict access to Pod product running in namespace dev.
Only allow the following Pods to connect to Pod products-service:
1. Pods in the namespace qa
2. Pods with label environment: stage, in any namespace

**Answer:**

Explanation:

```
$ k get ns qa --show-labels
NAME STATUS AGE LABELS
qa Active 47m env=stage
$ k get pods -n dev --show-labels
NAME READY STATUS RESTARTS AGE LABELS
product 1/1 Running 0 3s env=dev-team
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
name: restricted-policy
namespace: dev
spec:
podSelector:
matchLabels:
env: dev-team
policyTypes:
- Ingress
ingress:
- from:
- namespaceSelector:
matchLabels:
env: stage
- podSelector:
matchLabels:
env: stage
[desk@cli] $ k get ns qa --show-labels
NAME STATUS AGE LABELS
qa Active 47m env=stage
[desk@cli] $ k get pods -n dev --show-labels
NAME READY STATUS RESTARTS AGE LABELS
product 1/1 Running 0 3s env=dev-team
[desk@cli] $ vim netpol2.yaml
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
name: restricted-policy
namespace: dev
spec:
podSelector:
matchLabels:
env: dev-team
policyTypes:
- Ingress
ingress:
- from:
- namespaceSelector:
matchLabels:
env: stage
- podSelector:
matchLabels:
env: stage
```

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

**NEW QUESTION # 51**
SIMULATION
Enable audit logs in the cluster, To Do so, enable the log backend, and ensure that
1. logs are stored at /var/log/kubernetes/kubernetes-logs.txt.
2. Log files are retained for 5 days.
3. at maximum, a number of 10 old audit logs files are retained.
Edit and extend the basic policy to log:
1. Cronjobs changes at RequestResponse
2. Log the request body of deployments changes in the namespace kube-system.
3. Log all other resources in core and extensions at the Request level.
4. Don't log watch requests by the "system:kube-proxy" on endpoints or

- A. Send us the Feedback on it.

**Answer: A**

**NEW QUESTION # 52**
You suspect that the Kubernetes binaries on your cluster nodes may have been tampered with. Implement a process to verify the integrity of the binaries and identify any potential compromises.

**Answer:**

Explanation:
Solution (Step by Step):
1. Establish a known-good baseline: Obtain known-good copies of the Kubernetes binaries from a trusted source, such as the official Kubernetes release page or your distribution's package repository.
2. Calculate checksums: Calculate the SHA-256 checksums of the known-good binaries and the binaries on your nodes.
bash

```
sha256sum /usr/bin/kubeadm lusr/bin/kubelet 'usr/bin/kubectl
```

3. Compare checksums: Compare the checksums of the binaries on your nodes with the checksums of the known-good binaries. Any discrepancies indicate potential tampering.
4. Inspect binaries for modifications: If checksum mismatches are found, use tools like 'diff or 'cmp' to compare the suspect binaries with the known- good binaries to identify specific modifications.
5. Analyze system logs: Review system logs, such as audit logs and syslog, for any suspicious activity related to the Kubernetes binaries or processes.
6. Reinstall binaries from a trusted source: If tampering is confirmed, reinstall the Kubernetes binaries from a trusted source.
7. Investigate the root cause: Conduct a thorough investigation to determine the root cause of the tampering and take steps to prevent future compromises. This may involve reviewing access controls, network security, and security monitoring practices.

**NEW QUESTION # 53**
......

- Latest CKS Exam Question □ CKS Practice Test □ New CKS Test Cram □ Open website ➽ www.vce4dumps.com □ and search for ➽ CKS □ for free download □CKS Valid Test Testking
- Free PDF Quiz 2026 Pass-Sure CKS: Certified Kubernetes Security Specialist (CKS) New Dumps □ Search for ✔ CKS □✔□ and obtain a free download on ⇛ www.pdfvce.com ⇚ □New CKS Test Vce Free
- Free PDF 2026 Linux Foundation Valid CKS: Certified Kubernetes Security Specialist (CKS) New Dumps □ Immediately open ➥ www.testkingpass.com □ and search for [ CKS ] to obtain a free download ⏲Valid Dumps CKS Ebook
- Exam CKS Tutorial □ Practice CKS Test Online □ Authentic CKS Exam Questions □ Search for 「 CKS 」 and easily obtain a free download on ➡ www.pdfvce.com □□□ □New CKS Test Vce Free
- Free PDF Quiz 2026 Pass-Sure CKS: Certified Kubernetes Security Specialist (CKS) New Dumps □ Open 【 www.torrentvce.com 】 and search for ☀ CKS □☀□ to download exam materials for free □Authentic CKS Exam Questions
- Authentic CKS Exam Questions □ Exam CKS Simulator Fee □ Authentic CKS Exam Questions □ Immediately open 「 www.pdfvce.com 」 and search for ☀ CKS □☀□ to obtain a free download □CKS Practical Information
- CKS New Dumps - High-quality Linux Foundation Certified Kubernetes Security Specialist (CKS) - Latest CKS Exam Online □ Download 「 CKS 」 for free by simply entering ➽ www.exam4labs.com □ website □CKS Reliable Test Question
- Reliable CKS Test Experience □ Exam CKS Tutorial □ CKS Reliable Test Question □ ➠ www.pdfvce.com □ is best website to obtain ➡ CKS □□□ for free download □CKS New Test Bootcamp
- 100% Pass Quiz 2026 Perfect Linux Foundation CKS: Certified Kubernetes Security Specialist (CKS) New Dumps □ Search for 《 CKS 》 on ➤ www.practicevce.com □ immediately to obtain a free download □CKS Valid Test Testking
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, ncon.edu.sa, www.stes.tyc.edu.tw, pixabay.com, 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, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

BTW, DOWNLOAD part of PDFBraindumps CKS dumps from Cloud Storage: https://drive.google.com/open?id=1FOhQMk8diXcS-PX2S1NT4y-hOH5RB3tA