CKS시험문제집 & CKS최신시험대비공부자료

참고: KoreaDumps에서 Google Drive로 공유하는 무료, 최신 CKS 시험 문제집이 있습니다: https://drive.google.com/open?id=1CvKAHtm80qdqT0UBaTpCQGs96frjzL8o

KoreaDumps의Linux Foundation CKS시험자료의 문제와 답이 실제시험의 문제와 답과 아주 비슷합니다. 우리의 짧은 학습가이드로 빠른 시일 내에 관련지식을 터득하여 응시준비를 하게 합니다. 우리는 우리의Linux Foundation CKS인증시험덤프로 시험패스를 보장합니다.

CKS 시험은 Kubernetes 클러스터를 보안하는 능력을 시험하는 실습 중심 시험입니다. 이 시험은 Kubernetes 관리자가 직면할 수 있는 실제 상황을 시뮬레이션하는 17개의 시나리오로 구성되어 있습니다. 이러한 시나리오는 응시자의 Kubernetes 보안 개념 이해, 일반적인 취약점을 파악하고 완화하는 능력, Kubernetes 클러스터 보안을 위한 최상의 방법론에 대한 지식을 시험하는 것을 목적으로 설계되었습니다. 이 시험은 온라인으로 진행되며 전 세계 어디서든 응시할 수 있습니다. 응시자는 시험을 통과하여 2년간 유효한 CKS 자격증을 획득해야 합니다.

CKS 시험은 2 시간 이내에 완료 해야하는 15-20 개의 성능 기반 작업으로 구성된 엄격한 평가입니다. 시험은 온라인으로 수행되며 응시자는 명령 줄 도구 및 Kubernetes API 객체에 대한 지식뿐만 아니라 Kubernetes 클러스터에 액세스해야합니다. 인증은 2 년 동안 유효하며 재 인증 시험을 통과하거나 지속적인 교육 학점을 취득하여 갱신 할 수 있습니다.

>> CKS시험문제집 <<

CKS최신 시험대비 공부자료 & CKS시험대비 덤프데모

Linux Foundation업계에 종사하시는 분들은 CKS인증시험을 통한 자격증취득의 중요성을 알고 계실것입니다. KoreaDumps에서 제공해드리는 인증시험대비 고품질 덤프자료는 제일 착한 가격으로 여러분께 다가갑니다. KoreaDumps덤프는 CKS인증시험에 대비하여 제작된것으로서 높은 적중율을 자랑하고 있습니다.덤프를 구입하시면 일년무료 업데이트서비스, 시험불합격시 덤프비용환불 등 퍼펙트한 서비스도 받을수 있습니다.

최신 Kubernetes Security Specialist CKS 무료샘플문제 (Q14-Q19):

질문 # 14
You can switch the cluster/configuration context using the following command:
[desk@cli] $ kubectl config use-context stage
Context:
A PodSecurityPolicy shall prevent the creation of privileged Pods in a specific namespace.
Task:
1. Create a new PodSecurityPolcy named deny-policy, which prevents the creation of privileged Pods.
2. Create a new ClusterRole name deny-access-role, which uses the newly created PodSecurityPolicy deny-policy.
3. Create a new ServiceAccount named psd-denial-sa in the existing namespace development.
Finally, create a new ClusterRoleBindind named restrict-access-bind, which binds the newly created ClusterRole deny-access-role to the newly created ServiceAccount psp-denial-sa

정답：

설명：
Create psp to disallow privileged container
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
name: deny-access-role
rules:
- apiGroups: ['policy']
resources: ['podsecuritypolicies']
verbs: ['use']
resourceNames:
- "deny-policy"
k create sa psp-denial-sa -n development
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
name: restrict-access-bing
roleRef:
kind: ClusterRole
name: deny-access-role
apiGroup: rbac.authorization.k8s.io
subjects:
- kind: ServiceAccount
name: psp-denial-sa
namespace: development
Explanation
master1 $ vim psp.yaml
apiVersion: policy/v1beta1
kind: PodSecurityPolicy
metadata:
name: deny-policy
spec:
privileged: false # Don't allow privileged pods!
seLinux:
rule: RunAsAny
supplementalGroups:
rule: RunAsAny
runAsUser:
rule: RunAsAny
fsGroup:
rule: RunAsAny
volumes:
- '*'
master1 $ vim cr1.yaml
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
name: deny-access-role
rules:
- apiGroups: ['policy']
resources: ['podsecuritypolicies']
verbs: ['use']
resourceNames:
- "deny-policy"
master1 $ k create sa psp-denial-sa -n development
master1 $ vim cb1.yaml
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:

name: restrict-access-bing
roleRef:
kind: ClusterRole
name: deny-access-role
apiGroup: rbac.authorization.k8s.io
subjects:
Authorize specific service accounts:
- kind: ServiceAccount
name: psp-denial-sa
namespace: development
master1 $ k apply -f psp.yaml master1 $ k apply -f cr1.yaml master1 $ k apply -f cb1.yaml Reference: https://kubernetes.io/docs/concepts/policy/pod-security-policy/ master1 $ k apply -f cr1.yaml master1 $ k apply -f cb1.yaml master1 $ k apply -f psp.yaml master1 $ k apply -f cr1.yaml master1 $ k apply -f cb1.yaml Reference: https://kubernetes.io/docs/concepts/policy/pod-security-policy/

질문 # 15
You are responsible for securing the software supply chain of your company's applications deployed in a Kubernetes cluster. You are implementing a CI/CD pipeline that builds, tests, and deploys container images. Currently, your pipeline relies on pulling images directly from Docker Hub without any security checks. How would you enhance your pipeline to verify the integrity of the images pulled from Docker Hub?

정답：

설명：
Solution (Step by Step):
1. Implement Image Signing:
- Step I: Generate a signing key and certificate pair for your organization.
- Step 2: Configure your CIICD pipeline to sign container images after they are built using the generated key and certificate.
- Step 3: Configure your Kubernetes cluster to only pull and deploy images that are signed with your organization's certificate. This step involves creating a 'PodSecurityPoIicy' (PSP) or 'PodSecurityAdmissioru (PSA) resource to enforce image signing.
Example Code:
Example Code: 2. Integrate SBOM Generation: - Step 1: Configure your CI/CD pipeline to generate a Software Bill of Materials (SBOM) for each container image. - Step 2: Store the SBOM alongside the container image in your artifact repository. - Step 3: Implement a process to verify the SBOM against a vulnerability database to ensure the image does not contain any known vulnerabilities. Example Code: # Example of generating an SBOM with Syft syn packages my-image.tar 3. Utilize Container Scanning Tools: - Step 1: Integrate container scanning tools like Clair, Anchore, or Trivy into your CI/CD pipeline. - Step 2: Configure these tools to scan images before deployment for known vulnerabilities. - Step 3: Configure your pipeline to fail the build if vulnerabilities are detected. Example Code: # Example of scanning a container image with Trivy trivy image my-image:latest By implementing these security measures, you can significantly strengthen your software supply chain, reducing the risk ot vulnerabilities and malicious attacks.

질문 # 16
Create a PSP that will only allow the persistentvolumeclaim as the volume type in the namespace restricted.
Create a new PodSecurityPolicy named prevent-volume-policy which prevents the pods which is having different volumes mount apart from persistentvolumeclaim.
Create a new ServiceAccount named psp-sa in the namespace restricted.
Create a new ClusterRole named psp-role, which uses the newly created Pod Security Policy prevent-volume-policy
Create a new ClusterRoleBinding named psp-role-binding, which binds the created ClusterRole psp-role to the created SA psp-sa.
Hint:
Also, Check the Configuration is working or not by trying to Mount a Secret in the pod maifest, it should get failed.
POD Manifest:
apiVersion: v1
kind: Pod
metadata:
name:
spec:
containers:
- name:

image:
volumeMounts:
- name:
mountPath:
volumes:
- name:
secret:
secretName:

정답：

설명：
apiVersion: policy/v1beta1
kind: PodSecurityPolicy
metadata:
name: restricted
annotations:
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' spec:
privileged: false
Required to prevent escalations to root.
allowPrivilegeEscalation: false
This is redundant with non-root + disallow privilege escalation,
but we can provide it for defense in depth.
requiredDropCapabilities:
- ALL
Allow core volume types.
volumes:
- 'configMap'
- 'emptyDir'
- 'projected'
- 'secret'
- 'downwardAPI'
Assume that persistentVolumes set up by the cluster admin are safe to use.
- 'persistentVolumeClaim'
hostNetwork: false
hostIPC: false
hostPID: false
runAsUser:
Require the container to run without root privileges.
rule: 'MustRunAsNonRoot'
seLinux:
This policy assumes the nodes are using AppArmor rather than SELinux.
rule: 'RunAsAny'
supplementalGroups:
rule: 'MustRunAs'
ranges:
Forbid adding the root group.
- min: 1
max: 65535
fsGroup:
rule: 'MustRunAs'
ranges:
Forbid adding the root group.
- min: 1
max: 65535
readOnlyRootFilesystem: false

질문 # 17
You are deploying a critical application that handles sensitive user dat
a. Your security policy mandates that only specific system calls are allowed for the application container You decide to use seccomp to enforce this policy- Design a seccomp profile that allows only the following system calls: 'read', 'write', 'open', 'close', 'stat', 'fstat' , 'Istat' , 'getpid', 'getuid', 'getgidS , and 'exit_group'.

정답：

설명：
Solution (Step by Step) :
1. Define the Seccomp Profile:
- Create a 'seccomp-json' file with the following content:
2. Apply the Seccomp Profile to the Container: - You can apply the seccomp profile to the container using the 'securitycontext' in your deployment or pod spec - Include the following configuration: - 'securityContext.seccompProfile.type: Locar - 'securitycontextseccompprofile.localsrc: seccomp.json'
3. Test and Verify: - Deploy the application with the seccomp profile. - Run the application and test its functionality- - Verify that the application operates as expected and does not attempt to perform system calls that are not allowed by the seccomp profile. - Use tools like 'straces to monitor the system calls made by the application to confirm that seccomp is enforcing the restrictions.

질문 # 18
You need to implement a container image vulnerability scanning solution within your Kubernetes cluster. You want to use an external vulnerability scanner API that provides information about vulnerabilities in container images- Explain how you would design and implement this solution.

정답：

설명：
Solution (Step by Step) :
1. choose Vulnerability Scanner:
- Select a reputable vulnerability scanner API that provides a comprehensive database and accurate information about container image vulnerabilities.
- Some options include Aqua Security, Anchore Engine, Snyk, Twistlock, and more.
- Choose a scanner with a suitable API interface for integration with your Kubernetes environment.
2. Implement a Scanner Service:
- Create a Kubernetes service that will communicate with your chosen vulnerability scanner API.
- This service will act as an intermediary between Kubernetes and the external scanner
- The service should be able to:
- Accept image details (registry, image name, tag) as input.
- Send requests to the scanner API to retrieve vulnerability information.
- Process the results from the scanner and format them for Kubernetes.
- (Optional) Store the scan results for future analysis and reporting.
3. Design Scanner Workflow:
- You can trigger scans using different methods:
- Automated Scanning: Implement a mechanism (e.g., a cron job or webhook triggered by image pushes) to automatically scan new images.
- On-Demand Scanning: Allow users to manually request image scans via a command line interface (CLI) or a user interface.
4. Integration with Kubernetes:
- You can integrate your scanner service with Kubernetes using several approaches:
- Admission Webh00k1 Use a wet)h00k to intercept pod creation or updates. The webh00k can send the image details to your scanner service and block pod creation if critical vulnerabilities are detected.
- Custom Resource Definitions (CRDs): Create CRDs to manage image scanning tasks- You can define a "ImageScan" or "Vulnerabilityscan" resource that represents a scan request.
- Deployment Controller: Use a custom controller or operator to manage the scanning process. This allows you to define rules for automatic scanning
and integrate with other Kubernetes resources.
5. Scanner Service Implementation (Example):
- Here's a simplified example using Python and a hypothetical "vulnerability-scanner" APC
python
import requests
import json

6. Handle Scan Results: - After scanning, process the vulnerability information received from the API. - You can: - Store the scan results in a database or log file. - Generate alerts or reports based on the severity of vulnerabilities found. - Integrate with other security tools or dashboards for analysis and remediation.

질문 # 19
.....

경쟁율이 점점 높아지는 IT업계에 살아남으려면 국제적으로 인증해주는 IT자격증 몇개쯤은 취득해야 되지 않을가요? Linux Foundation CKS시험으로부터 자격증 취득을 시작해보세요. Linux Foundation CKS 덤프의 모든 문제를 외우기만 하면 시험패스가 됩니다. Linux Foundation CKS덤프는 실제 시험문제의 모든 유형을 포함되어있어 적중율이 최고입니다.

CKS최신 시험대비 공부자료: https://www.koreadumps.com/CKS_exam-braindumps.html

- CKS시험문제집 덤프구매후 60일내 주문은 불합격시 환불가능 □ 오픈 웹 사이트✔ kr.fast2test.com □✔□검색《 CKS 》무료 다운로드CKS시험패스 가능 공부자료
- 시험대비 CKS시험문제집 최신버전 덤프샘플 문제 □ { www.itdumpskr.com }에서[CKS]를 검색하고 무료로 다운로드하세요CKS퍼펙트 최신버전 문제
- CKS시험대비덤프 □ CKS퍼펙트 최신버전 덤프자료 □ CKS높은 통과율 덤프샘플 다운 □ ➡ www.dumptop.com □□□의 무료 다운로드⇛ CKS ⇚페이지가 지금 열립니다CKS시험대비 덤프 최신 데모
- 퍼펙트한 CKS시험문제집 덤프 샘플문제 다운 □ 【 www.itdumpskr.com 】에서 검색만 하면✔ CKS □✔□를 무료로 다운로드할 수 있습니다CKS Vce
- 시험대비 CKS시험문제집 최신버전 덤프샘플 문제 ✈ （ www.pass4test.net ）웹사이트에서□ CKS □를 열고 검색하여 무료 다운로드CKS최신 업데이트 시험대비자료
- CKS퍼펙트 덤프샘플 다운로드 □ CKS최신 업데이트 시험덤프문제 □ CKS시험대비 최신 덤프 □ [www.itdumpskr.com]에서✔ CKS □✔□를 검색하고 무료로 다운로드하세요CKS퍼펙트 최신버전 덤프자료
- CKS시험문제집 덤프구매후 60일내 주문은 불합격시 환불가능 □ 《 kr.fast2test.com 》웹사이트에서□ CKS □를 열고 검색하여 무료 다운로드CKS인증덤프문제
- 높은 통과율 CKS시험문제집 시험자료 □ { www.itdumpskr.com }에서《 CKS 》를 검색하고 무료 다운로드 받기CKS시험패스 가능한 인증공부자료
- CKS최고덤프 □ CKS높은 통과율 덤프샘플 다운 □ CKS최신 업데이트 시험대비자료 □ 검색만 하면☀ www.pass4test.net □☀□에서☀ CKS □☀□무료 다운로드CKS시험대비덤프
- CKS퍼펙트 최신버전 문제 □ CKS퍼펙트 최신버전 문제 □ CKS시험덤프데모 ✡ 지금（ www.itdumpskr.com ）을(를) 열고 무료 다운로드를 위해「 CKS 」를 검색하십시오CKS시험준비공부
- CKS Vce □ CKS Vce □ CKS최신 업데이트버전 인증덤프 □ { www.exampassdump.com }에서□ CKS □를 검색하고 무료 다운로드 받기CKS최신 업데이트 시험덤프문제
- 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, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, knowyourmeme.com, Disposable vapes

그리고 KoreaDumps CKS 시험 문제집의 전체 버전을 클라우드 저장소에서 다운로드할 수 있습니다: https://drive.google.com/open?id=1CvKAHtm80qdqT0UBaTpCQGs96frjzL8o