Training: The Linux Foundation
CKS Certified Kubernetes Security Specialist

THE LINUX FOUNDATION AUTHORIZED TRAINING PARTNER

TRAINING GOALS:

The Certified Kubernetes Security Specialist (CKS) program provides assurance that a CKS has the skills, knowledge, and competence on a broad range of best practices for securing container-based applications and Kubernetes platforms during build, deployment and runtime. CKA certification is required to sit for this exam.

Who Is It For:

A Certified Kubernetes Security Specialist (CKS) is an accomplished Kubernetes practitioner (must be CKA certified) who has demonstrated competence on a broad range of best practices for securing container-based applications and Kubernetes platforms during build, deployment and runtime.

About This Certification:

CKS is a performance-based certification exam that tests candidates' knowledge of Kubernetes and cloud security in a simulated, real world environment. Candidates must have taken and passed the Certified Kubernetes Administrator (CKA) exam prior to attempting the CKS exam. CKS may be purchased but not scheduled until CKA certification has been achieved.

CKA Certification must be active (non-expired) on the date the CKS exam (including Retakes) is scheduled.

What It Demonstrates:

Obtaining a CKS demonstrates a candidate possesses the requisite abilities to secure container-based applications and Kubernetes platforms during build, deployment and runtime, and is qualified to perform these tasks in a professional setting.

CONSPECT:

Domains & Competencies:

- **Cluster Setup10%**
  - Use Network security policies to restrict cluster level access
  - Use CIS benchmark to review the security configuration of Kubernetes components (etcd, kubelet, kubedns, kubeapi)
  - Properly set up Ingress objects with security control

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Protect node metadata and endpoints
- Minimize use of, and access to, GUI elements
- Verify platform binaries before deploying

- **Cluster Hardening15%**
  - Restrict access to Kubernetes API
  - Use Role Based Access Controls to minimize exposure
  - Exercise caution in using service accounts e.g. disable defaults, minimize permissions on newly created ones
  - Update Kubernetes frequently
- **System Hardening15%**
  - Minimize host OS footprint (reduce attack surface)
  - Minimize IAM roles
  - Minimize external access to the network
  - Appropriately use kernel hardening tools such as AppArmor, seccomp
- **Minimize Microservice Vulnerabilities20%**
  - Setup appropriate OS level security domains e.g. using PSP, OPA, security contexts
  - Manage Kubernetes secrets
  - Use container runtime sandboxes in multi-tenant environments (e.g. gvisor, kata containers)
  - Implement pod to pod encryption by use of mTLS
- **Supply Chain Security20%**
  - Minimize base image footprint
  - Secure your supply chain: whitelist allowed registries, sign and validate images
  - Use static analysis of user workloads (e.g.Kubernetes resources, Docker files)
  - Scan images for known vulnerabilities
- **Monitoring, Logging and Runtime Security20%**
  - Perform behavioral analytics of syscall process and file activities at the host and container level to detect malicious activities
  - Detect threats within physical infrastructure, apps, networks, data, users and workloads
  - Detect all phases of attack regardless where it occurs and how it spreads
  - Perform deep analytical investigation and identification of bad actors within environment
  - Ensure immutability of containers at runtime
  - Use Audit Logs to monitor access

This exam is an online, proctored, performance-based test that requires implementing multiple solutions within a Remote Desktop Linux environment. Visual Studio Code, Vim and Webstorm (kindly sponsored by JetBrains) are included as editors in this environment.

The exam includes tasks simulating on-the-job scenarios, and Candidates have 2 hours to complete

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

the tasks

- Candidate Handbook
- Tips Document
- FAQ
- Linux Foundation Global Certification & Confidentiality Agreement

REQUIREMENTS:

- Active (non-expired) CKA certification is a prerequisite for this exam.

Difficulty level



Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007