Training: The Linux Foundation
CKA Certified Kubernetes Administrator + CKS Certified Kubernetes Security Specialist Exam Bundle

TRAINING GOALS:

A certified K8s administrator has demonstrated the ability to do basic installation as well as configuring and managing production-grade Kubernetes clusters. They will have an understanding of key concepts such as Kubernetes networking, storage, security, maintenance, logging and monitoring, application lifecycle, troubleshooting, API object primitives and the ability to establish basic use-cases for end users. 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.

The CKA was created by The Linux Foundation and the Cloud Native Computing Foundation (CNCF) as a part of their ongoing effort to help develop the Kubernetes ecosystem. The exam is an online, proctored, performance-based test that requires solving multiple tasks from a command line running Kubernetes.

The 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.

Who Is It For

The CKA certification is for Kubernetes administrators, cloud administrators and other IT professionals who manage Kubernetes instances. 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.

CKA Domains & Competencies

- Storage 10%
  - Understand storage classes, persistent volumes
  - Understand volume mode, access modes and reclaim policies for volumes
  - Understand persistent volume claims primitive
  - Know how to configure applications with persistent storage
- Troubleshooting 30%

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 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

- Evaluate cluster and node logging
- Understand how to monitor applications
- Manage container stdout & stderr logs
- Troubleshoot application failure
- Troubleshoot cluster component failure
- Troubleshoot networking

- Workloads & Scheduling 15%
  - Understand deployments and how to perform rolling update and rollbacks
  - Use ConfigMaps and Secrets to configure applications
  - Know how to scale applications
  - Understand the primitives used to create robust, self-healing, application deployments
  - Understand how resource limits can affect Pod scheduling
  - Awareness of manifest management and common templating tools

- Cluster Architecture, Installation & Configuration 25%
  - Manage role based access control (RBAC)
  - Use Kubeadm to install a basic cluster
  - Manage a highly-available Kubernetes cluster
  - Provision underlying infrastructure to deploy a Kubernetes cluster
  - Perform a version upgrade on a Kubernetes cluster using Kubeadm
  - Implement etcd backup and restore

- Services & Networking 20%
  - Understand host networking configuration on the cluster nodes
  - Understand connectivity between Pods
  - Understand ClusterIP, NodePort, LoadBalancer service types and endpoints
  - Know how to use Ingress controllers and Ingress resources
  - Know how to configure and use CoreDNS
  - Choose an appropriate container network interface plugin

CKS Domains & Competencies

- Cluster Setup 10%
  - 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 Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 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 Hardening 15%
  - 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 Hardening 15%
  - 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 Vulnerabilities 20%
  - 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 Security 20%
  - 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

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 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

Exam Details & Resources

Both the CKA and CKS exams are online, proctored, performance-based tests that requires solving multiple tasks from a command line running Kubernetes. For each exam, candidates have 2 hours to complete the tasks.

The CKA exam is based on Kubernetes v1.25
The CKS exam is based on Kubernetes v1.25

The CKS & CKA exam environments will be aligned with the most recent K8s minor version within approximately 4 to 8 weeks of the K8s release date

Certified Kubernetes Security Specialist (CKS) 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.

Please review the Candidate Handbook, Curriculum Overview and Exam Tips along with other recommended resources below.

- Candidate Handbook
- Exam Tips
- Curriculum Overview
- Frequently Asked Questions
- Verify Certification
- CKA Reseller FAQs
- Linux Foundation Global Certification and Confidentiality Agreement

Difficulty level

CERTIFICATE:

After passing the exams, candidates will receive the Certified Kubernetes Administrator (CKA) + the Certified Kubernetes Security Specialist (CKS) certificates in pdf form.

ADDITIONAL INFORMATION:

CKA Exam Includes

- Proctored Online Exam Delivery

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 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

- Exam Duration 2 Hours
- Certification Valid for 3 Years
- 12 Month Exam Eligibility
- Free Retake
- PDF Certificate and Digital Badge
- Software Version: Kubernetes v1.25
- Performance-Based Exam
- Exam Simulator

CKS Exam Includes

- Proctored Online Exam Delivery
- Exam Duration 2 Hours
- Certification Valid for 2 Years
- 12 Month Exam Eligibility
- Free Retake
- PDF Certificate and Digital Badge
- Software Version: Kubernetes v1.25
- Performance-Based Exam
- Exam Simulator

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 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