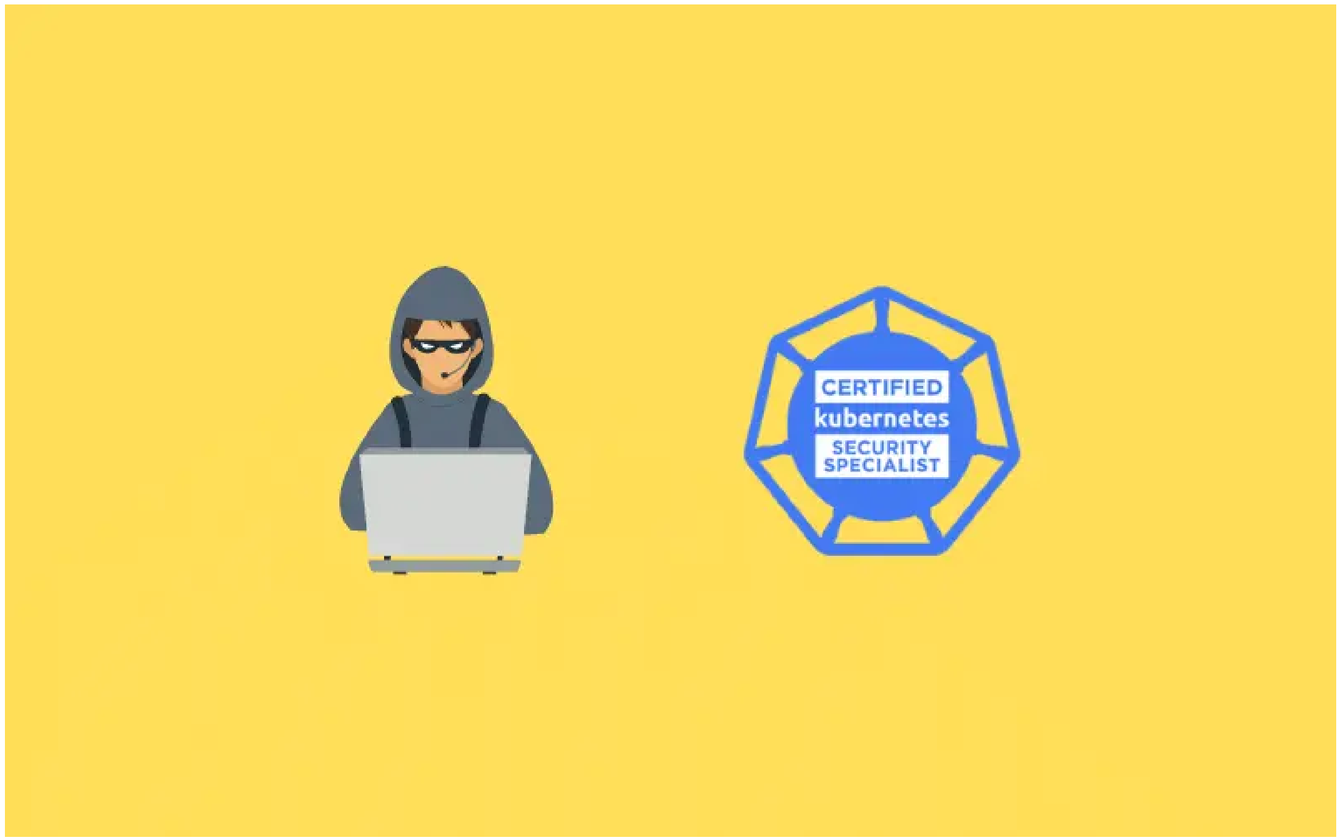
K — KUBERNETES

# CKS Exam Study Guide: Resources to Pass Certified Kubernetes Security Specialist

by **Bibin Wilson** · June 23, 2021




In this Certified Kubernetes Security Specialist (CKS) Exam study guide, I have listed all the resources you can use to pass the CKS certification exam.

## What Is the Certified Kubernetes Security Specialist Exam?

The official CNCF certification page says,

> 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.

The CKS exam curriculum is well structured, with topics related to Kubernetes security. In fact, you can use the curriculum as a checklist for your existing Kubernetes implementations.

## Registering For CKS Exam [Save $57]

Your first step towards CKS Certification is registering for the exam on the Linux Foundation portal.

> **Note:** Save $57 Today on CKA|CKAD|CKS certification using the Voucher code given below. This offer expires soon.

**SAVE $57 ON CKS TODAY**

**Exam Voucher:** Use coupon **SCOFFER15** at checkout

Here is what your should know about the CKS exam registration.

1. From the day of registration, you have one year time to schedule and appear for the CKS certification exam
2. You get a total of 2 free attempts to pass the certification. However, if you miss the scheduled exam, you don't get the free retake.

## Certified Kubernetes Security Specialist (CKS) Exam Preparation Guide

We will look at the detailed CKS resources list and links to the official documentation you could use during the CKS exam.

CKS GUIDE TOPICS



---

# CKS Exam Prerequisites

The only prerequisite is that you should have a **valid CKA certification** to sit for the CKS Exam.

If you have not passed the CKA exam, refer to our CKA exam guide for all useful resources.

Even if you don't have the CKA certification, you can purchase the CKS exam as a bundle (CKA + CKS). You can save up to $206 using the bundle with an additional 21% discount. However, you need to first pass the CKS and then you can appear for the CKS exam.

# CKS Exam Details

Following are the important information about CKS Exam.

| | |
|---|---|
| Exam Duration | 2 hrs |
| Pass Percentage | 67% |
| Kubernetes Version | v1.20 |
| CKS Validity | 2 Years |
| CKS Certification Exam Cost | $300 |

As CKS is an open book exam, you can use the following Kubernetes and third-party tools documentation that is part of the CKS exam.

## Kubernetes Documentation

1. https://kubernetes.io/docs/home/
2. https://github.com/kubernetes/

### Allowed Third-Party Tools & Documentation for CKS exam

> **Important Note:** The following domains are allowed in the exam. However, you are not allowed to visit any other domains that are mentioned in the documents.

1. https://github.com/aquasecurity/trivy
2. https://docs.sysdig.com/
3. https://falco.org/docs/
4. https://gitlab.com/apparmor/apparmor/-/wikis/Documentation

Please refer the official Kubernetes exam FAQ section for more details

## CKS Exam Syllabus

CKS Exam aims to test your skills on different security aspects. The following table shows the different domains and their weightage for the CKS certification.

| Topic | Weightage |
|---|---|
| Cluster Setup | 10% |
| Cluster Hardening | 15% |
| System Hardening | 15% |
| Minimize Microservice Vulnerabilities | 20% |
| Supply Chain Security | 20% |
| Monitoring, Logging, and Runtime Security | 20% |

## Certified Kubernetes Security Specialist Certification Courses

If you want to sign up for a course for your CKS preparation, the following are the courses you will ever need.

1. CKS Course by Kim Wüstkamp with Exam Simulator

Both authors have done a great job creating the course content with good practice labs.

## Kubernetes Security Books

Following are the Kubernetes books related to security you can use of CKS preparation.

1. Container Security by Liz Rice
2. Kubernetes Security by Liz Rice

## Setting up CKS Practice Labs

It would be best to have a practice cluster to learn and try out all the concepts involved in CKS certification. I have the following suggestion for CKS practice labs.

1. Katacoda
2. Minikube
3. Kubernetes Setup using Kubeadm [Detailed Guide]
4. Kubernetes Vagrant Setup using Kubeadm
5. GKE Cluster using free Google Cloud Credits
6. EKS Service on AWS using Free tier program
7. AKS service on Azure using free cloud credits
8. Kubernetes Cluster on Digital Ocean[ Get $100 Digital Ocean Free Credits]

> **Note**: To get notification on the above-mentioned setup and other CKS tutorial articles, Signup to the CKS newsletter

## CKS Syllabus Wise Resources

Let's have a look at the official syllabus-wise resources for the CKS exam. All the topics mentioned are as per the official Linux Foundation Certified Kubernetes Security Specialist Exam Syllabus.

## Cluster Setup [10%]

Under cluster setup, the focus is more on the security aspects of the cluster

## Kubernetes Network Policies

By default, when you set up a Kubernetes cluster, pods in all the namespaces can talk to each other.

This is not a secure setup because you might be running a different type of workload in a cluster that requires isolation in terms of networking.

Kubernetes network policies help you to enable rules for pod network communication.

| | |
|---|---|
| Use Network security policies to restrict cluster level access | Kubernetes Network Security Policy Documentation |
| Associated Task | Declaring Kubernetes Network Policy |
| Network Policy Editor | editor.cilium.io |

## Kubernetes CIS benchmark

Center for Internet Security (CIS) with the Kubernetes community has created the benchmarks for Kubernetes security standards.

Organizations can use the Kubernetes CIS benchmarks to achieve the security and compliance requirements.

If you want to know more about CIS, please read CIS FAQ's

See Kubernetes CIS benchmark to download the latest CIS benchmarks for kubernetes.

Kube-bench is an open-source utility maintained by Aquasec to run all the CIS benchmark checks against a Kubernetes cluster.

| | |
|---|---|
| Use CIS benchmark to review the security configuration of Kubernetes components (etcd, kubelet, kubedns, kubeapi) | CIS Kubernetes benchmark using Kube-bench |

## Ingress Security

From a security standpoint, for Ingress, the primary focus is on configuring ingress with TLS configurations

Also, it would help if you looked at setting up the namespaces scoped and cluster

You should also look at setting up multiple ingress/ingress controllers using the Ingressclass

| | |
|---|---|
| Properly set up Ingress objects with security control | Ingress documentation |

## Kubernetes Node Metadata & Endpoints

Metadata concealment is required for cloud-based Kubernetes setup where the instances expose the instance metadata information, including credentials.

This means the pods running on each instance would have access to the metadata server endpoint to retrieve information.

Pod's access to the Metadata server can be controlled via Network policies.

| | |
|---|---|
| Protect nod e metadata and endpoints | Restricting cloud metadata API access |
| Configuring Network Policies | Guide to configure network policies |

**Note:** When you use managed Kubernetes services on the cloud (GKE, EKS, AKS), it comes with options to disable metadata access for pods.

## Securing Kubernetes GUI

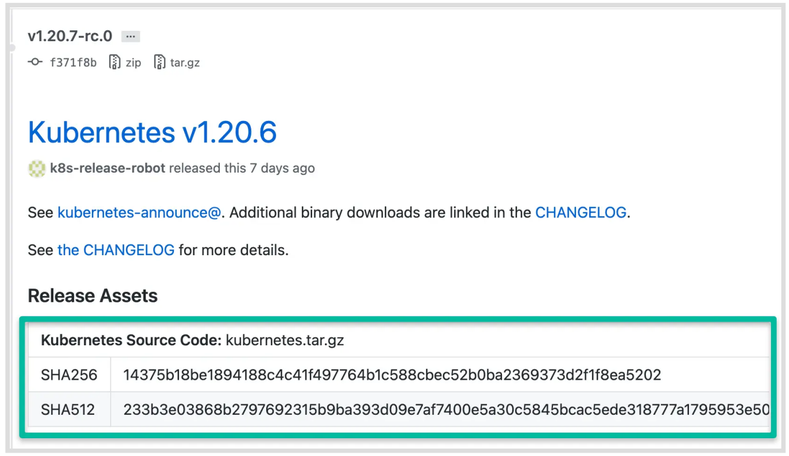
It is essential to secure Kubernetes dashboard access as it is accessed by cluster users from different networks in an organization. Also, many Kubernetes hacking incidents happened due to the wrong security configurations of the Kubernetes dashboard.

You need to learn all the best practices and configurations involved in setting up a secure Kubernetes dashboard. For example, limiting access to the dashboard with specific internal networks, user access with limited privileges to the dashboards, etc.

| | |
|---|---|
| Minimize use of, and access to, GUI elements | Kubernetes Web UI Configurations |
| Blog on Securing Kubernetes Dashboard | How to Secure Kubernetes Dashboard |

Learn to verify the Kubernetes binaries using the checksum. The kubernetes Github release page has the version numbers and SHA ids to verify the binary.

| | |
|---|---|
| Kubernetes Binaries | Github Kubernetes Releases |




# Cluster Hardening [15%]

Kubernetes Cluster Hardening **carries 15% weightage** in the CKS exam. Let's have a look at the individual concepts under cluster hardening.

## Restrict access to Kubernetes API

Restricting API access is very important when it comes to Kubernetes Production Implementation. Third-party services and services running inside the cluster should access the Kubernetes API with only required privileges.

The primary topics under this section would be bootstrap tokens, RBAC, ABAC, service account, and admission webhooks.

| | |
|---|---|
| Cluster API access methods | Ways to access Kubernetes cluster API |
| Kubernetes API Access Security | Controlling access to Kubernetes API |
| Authentication | Kubernetes Authentication Overview |
| Authorization | Kubernetes Authorization Overview |
| Admission Controllers | Admission Controllers Overview |
| Admission Webhooks | Admission Webhooks Overview |
| Certificates | Certificate Signing Requests Overview |
| Note Authorization | Node Authorization Overview |

## Use Role-Based Access Controls to minimize exposure

With Kubernetes RBAC, you can define fine-grained control on who can access the Kubernetes API to enforce the principle of least privilege. Allowing unnecessary cluster-wide access to everyone is a common mistake done during Kubernetes implementations.

Two main concepts in RBAC are,

1. **Role**: List of allowed API access
2. **RoleBinding** – Binding a role to a user, group, or service account.

| | |
|---|---|
| Roles, ClusterRoles, RoleBindings and ClusterRoleBindings | RBAC detailed documentation |
| | |

## Exercise caution in using service accounts e.g., disable defaults, minimize permissions on newly created ones.

Service accounts are the best way to provide access to application/pods which require Kubernetes API access.

Every namespace has a default service account, and it gets attached to the pod if you don't specify any service account explicitly. The default service account does not have any privileges. But if you bind a role to it, it will get all the access listed in the role, and it applies to all the pods in the namespace.

Standard practice is to deploy different workloads with different service accounts to enforce the principle of least privilege.

| | |
|---|---|
| Service Account | Service Account Management Guide |
| Task | Configure service account for a Pod |

## Update Kubernetes frequently

Whenever you upgrade a Kubernetes cluster, you should follow the recommended practices to make sure you have the application availablility.

Also, you should have mechanisms to validate the cluster components, security configurations, and application status post-upgrade.

| | |
|---|---|
| | Kubeadm |
| Task | Upgrade a cluster |

# System Hardening [15%]

System hardening aims at reducing vulnerabilities in applications and infrastructure components that reduce the attack surface.

The common system hardening activities are

1. Applying timely patches
2. Removing all non-essential utilities
3. Limiting access with firewall rules and utilities.
4. Logging all system activities.

When it comes to CKS, we have the following list of system hardening activities.

## Minimize host OS footprint (reduce attack surface)

1. Removing unwanted binaries and services that are not required for cluster operation.
2. Adding correct firewall rules to restrict host access on opened ports
3. Containers should have fewer privileges on the host OS. Run container as a non-root user

| | |
|---|---|
| Restricting Kernel Modules | Preventing Container Loading unwanted Kernel modules |

## Minimize IAM roles

This is to achieve the principle of least privilege.

Refer topic related to RBAC for role-related concepts. Normally IAM is applicable for cloud implementations that integrate with kubernetes RBAC

## Minimize external access to the network

Loadbalancer is a common components that allowed external access for Kubernetes cluster.

### Appropriately use kernel hardening tools such as AppArmor, seccomp

> **AppArmor** ("Application Armor") is a Linux kernel security module that allows the system administrator to restrict programs' capabilities with per-program profiles.

AppArmor is part of the official CKS allowed documentation.

| | |
|---|---|
| AppArmor | Restrict a Container's Access to Resources with AppArmor |
| Seccomp | Restrict a Container's Syscalls with Seccomp |
| Task | Securing a Pod Using Apparmor |
| Task | Set the Seccomp Profile for a Container |

## Minimize Microservice Vulnerabilities [20%]

As the title suggests, this section is more about service to service communications. You need to learn all the core concepts and Kubernetes objects involved in securing communication between pods.

### Setup appropriate OS-level security domains e.g. using PSP, OPA, security contexts

PSP is getting deprecated from Kubernetes version V1.21. But it is a good topic from a learning prespective.

Open Policy Agent is a great utility for implementing fine grained controls for microservices.

| | |
|---|---|
| PSP | Pod Security Policy |
| OPA | OPA Gatekeeper: Policy and Governance for Kubernetes |

## Manage Kubernetes secrets

Kubernetes secret is one of the ways to save sensitive information inside the pod. But, it is not encrypted. It is saved in a base64 encoded format. However, you can encrypt the data at rest.

| | |
|---|---|
| Kubernetes Secret | Kubernetes Secret Overview |
| Task | Distribute Credentials Securely Using Secrets |

## Use container runtime sandboxes in multi-tenant environments (e.g. gvisor, kata containers)

Kata Containers and gVisor helps in workload isolation. It can be implemented using the Kubernetes `RuntimeClass` where you can specify the required runtime for the workload.

| | |
|---|---|
| Pod Security Standards | Sandboxed Pods |
| Workload Isolation | Workload Isolation using gVisor and kata containers |

## Implement pod to pod encryption by use of mTLS

There is no documentation on enabling mTLS between pods. However, you can use the kubernetes `certificates.k8s.io` API to generate certificates to use in the pod to pod encryption.

For example, if you have two java services, you can convert the certificates you generate from the certificate API and convert it to JKS format using keytool and enable the pod to pod encryption with java settings.

| | |
|---|---|
| Task: Generating TLS Certificate | Manage TLS Certificates in a Cluster |

# Supply Chain Security [20%]

## Minimize base image footprint

There is no specific documentation on base image optimization on kubernetes.io. However, you can use following blog for learning purpose.

## Secure your supply chain: whitelist allowed registries, sign and validate images

It's important to verify the pulled base images are from valid sources. This can be achieved using `ImagePolicyWebhook` admission controller.

| | |
|---|---|
| ImagePolicyWebhook | Using ImagePolicyWebhook Admission Controller |

## Use static analysis of user workloads (e.g.Kubernetes resources, Docker files)

| | |
|---|---|
| Static analysis of user workloads | Statically Analyse YAML |
| | |

## Scan images for known vulnerabilities

Aquasec trivy is recommended in the Kubernetes CKS exam documentation. You can use Trivy to scan images for vulnerabilities.

| | |
|---|---|
| Trivy | Getting started with Trivy for vulnerability scanning. |
| | |

# 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

| | |
|---|---|
| Syscalls with Seccomp | Restrict a Container's Syscalls with Seccomp |

## Detect threats within a physical infrastructure, apps, networks, data, users, and workloads

Falco is the Kubernetes threat detection engine. It can alert find unexpected application behaviour and alert threats on time.

### Detect all phases of attack regardless of where it occurs and how it spreads

Falco might help here. Need to study more about it.

### Perform deep analytical investigation and identification of bad actors within the environment

Audit logging helps investigating issues in Kubernetes.

| | |
|---|---|
| Investigation | Impementing Kubernetes Auditing |

### Ensure immutability of containers at runtime

You can make the pods immutable by making everything the pod uses ReadOnly. For example, readonly filesystem, configmaps and secrtes.

| | |
|---|---|
| Immutable file system | PSP **readOnlyRootFilesystem** |

### Use Audit Logs to monitor access

Audit logs capture all the events associated with Kubernetes objects. The audit logs can be used by the monitoring systems to create alerts for unexpected actions.

| | |
|---|---|
| Kubernetes Auditing | Enabling Kubernetes Auditing |

## Conclusion

CKS is one of the sought-after certifications for DevOps engineers.

This is the ultimate guide to the Certified Kubernetes Security Specialist exam (CKS). I have covered the most important resources required to ace the CKS exam

If you plan to do the CKS certification, you should not aim to pass the certification with practice exams and exam dumps.

It would really help if you focused on learning all the core Kubernetes Security-

I will constantly be updating this CKS exam guide with useful resources and tips to pass the CKS exam. Also, I will be publishing a detailed blog on each topic in the syllabus.



## Get All The Other CKS Tutorial in Email

Email Address

SUBSCRIBE

**Note:** Please check you Inbox and confirm the subscription

(Check the Update/Spam folders if you dont find the email in Inbox)

**TAGS:** DevOps Certification

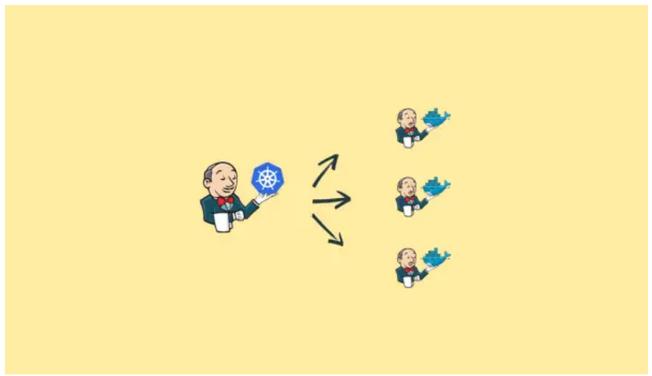


**Bibin Wilson**

An author, blogger and DevOps practitioner. In spare time, he loves to try out the latest open source technologies. He works as an Associate Technical Architect



YOU MAY ALSO LIKE



J — JENKINS

## How to Setup Jenkins Build Agents on Kubernetes Cluster

by **Bibin Wilson** · July 4, 2021

In this Jenkins tutorial, I explained the detailed steps to set up Jenkins master and scale Jenkins build...

K — KUBERNETES

## How to Setup Ingress on GKE using GKE Ingress Controller

by **devopscube** · June 24, 2021

This tutorial will guide you to setup Ingress on GKE using a GKE ingress controller that covers: The...

C — CI/CD

## How To Setup Jenkins On Kubernetes Cluster – Beginners Guide

by **Bibin Wilson** · May 9, 2021

Hosting Jenkins on a Kubernetes cluster is beneficial for Kubernetes-based deployments and dynamic container-based scalable Jenkins agents. In...

H — HOW TO

## How To Setup Grafana On Kubernetes

by **Bibin Wilson** · April 23, 2021

Grafana is an open-source lightweight dashboard tool. It can be integrated with many data sources like Prometheus, AWS...

K — KUBERNETES

## How to Create kubernetes Role for Service Account

by **Bibin Wilson** · June 1, 2021

In this blog, you will learn how to create Kubernetes role for a service account and use it...

K — KUBERNETES

## CKA Exam Study Guide: A Complete Resource For CKA Aspirants

by **Shishir Khandelwal** · June 25, 2021

This CKA Exam study guide will help you prepare for the Certified Kubernetes Administrator (CKA) exam with all...