StackRox

Certified Kubernetes Security Specialist Study Guide

Certified Kubernetes Security Specialist Study Guide

Author: Michael Foster, StackRox Cloud Native Advocate

Introduction

The Cloud Native Computing Foundation (CNCF) announced the Certified Kubernetes Security Specialist (CKS) certification is now generally available. This guide is designed to give you a starting point to understand the exam structure, topics, and exam-taking best practices. The guide will not provide you direct questions about the exam. Let's start by reviewing the exam structure by referencing the Linux Foundation documentation.

Exam Structure and Requirements

The CKS exam structure is:

- 2 hours long
- Require a passing score of 67%
- 15-20 performance-based tasks
- Uses Kubernetes version 1.19
- Cost $300 USD
- Free exam retake
- Certification valid for two years
- 12-month exam eligibility
- A valid CKA certificate is required

To take the CKS, applicants must already have a valid CKA certificate. If you have not taken the CKA we recommend completing the certificate before progressing to the CKS certification. The format of the CKS exam is almost identical to the CKA which helps if applicants are taking both tests in succession.

Exam Format

The Linux Foundation also outlined the exam format, and it is worth reading to help with exam expectations:

- Each task on this exam must be completed using a designated cluster/configuration context.
- Sixteen clusters comprise the exam environment, one for each task. Each cluster is made up of one master node and one worker node.
- At the start of each task, an infobox provides you with the cluster name/context and the master and worker node's hostname.
- You can switch the cluster/configuration context using a command such as the following: kubectl config use-context <cluster/context name>.
- Nodes making up each cluster can be reached via ssh, using a command such as the following: ssh <nodename>.
- You have elevated privileges on any node by default, so there is no need to assume elevated privileges.
- You must return to the base node (hostname CLI) after completing each task.
- Nested−ssh is not supported.
- You can use kubectl and the appropriate context to work on any cluster from the base node. When connected to a cluster member via ssh, you will only work on that cluster via kubectl.
- Further instructions for connecting to cluster nodes will be provided in the appropriate tasks.
- The CKS environment is currently running Kubernetes v1.19. (Quarterly exam updates are planned to match future Kubernetes releases).

Adding to the Linux Foundations format, there are a couple of extra notes to give more context.

- Vi/Vim is the default editor during the exam. If you require Gedit, Emacs, or Nano it will have to be installed in each node you work on.
- Vi/Vim is preconfigured for the correct tabs/spaces required to format YAML files.

With the context given, it is time to discuss how to prepare for the exam.

Preparing for the Exam

To help prepare for the CKS exam, StackRox has created a GitHub Repo that will create a Kubernetes cluster using version 1.19 and provide Kubernetes security tasks to evaluate your expertise. The repo also contains a full library of resources to help guide you through each section of the exam and outline the core Kubernetes security topics. Over the coming months, we will be updating the repo with various Kubernetes security concepts, topics, and creating new tasks to test your knowledge.

Getting Started

1. Register for the CKS at the Linux Foundation website.
2. Follow the guidelines to book your exam, and set a date on to three months in advance.
3. Read the complete Certified Kubernetes Security Specialist Study Guide.
4. Follow the Kubernetes Security Specialist Study Guide GitHub repository and review the other resources outlined in the README to a better understand the various concepts.

General Tips for the Exam

With learned lessons from the CKA exam, here are some general tips for dealing with the performance and task-based Kubernetes exams.

- Always review the Linux Foundations documentation. For frequently asked questions and any updates to the exam structure.
- Read each question carefully and manage the time accordingly. If a question asks for a pod, make sure to create a pod and not a deployment. The exam will evaluate based on the outputs to files and deployment/pod names. Errors in filenames/pods names may cause the question to be evaluated as incorrect.
- Bookmark and use any resources form the following domains and their respective subdomains:

  - Kubernetes Documentation
    - https://kubernetes.io/sdocs/
    - https://github.com/kubernetes/
    - https://kubernetes.io/blog/
  - Tools
    - Trivy documentation
    - Sysdig documentation
    - Falco documentation
    - AppArmor Documentation
- Recording task progression will help to prioritize where to spend the final moments during the exam. In previous exams, there is a notepad during the exam. In the new format, there is a progress bar and the ability to flag comments for a second look. One option is to use the flag ability to signal that you are completely finished with a question. With the other option of flagging questions, you are unsure of.
- Since time is of the essence, take advantage of the kubectl cheat sheet, and use aliases to cut down on kubectl typos.
- Be proficient in vi/vim for file editing during the test. Luckily, the spacing is preformatted for YAML files.
- Pay attention to the question context. There will be a context change command at the beginning of every question. Since there are 16 unique clusters, make sure to address the correct cluster to use time efficiently (and produce fewer headaches).
- Never write a YAML file from scratch. Use the –dry-run=client -o yaml > example.yaml to output example formats without submitting the commands to the cluster. With the new format, the YAML files are given to with its bare bones formatting. It will be up to you to understand how to populate and apply them. Use the files available as they will give you a better understanding of what is required of the question.

- Learn how to sort through JSON outputs. There may be a question where a search through active pods/ deployments for labels, memory limits, CPU limits, etc is required. Save a significant amount of time on a low-value question by sifting through objects efficiently.
- The exam will use kubeadm for creating the Kubernetes Cluster. Review the systemd basics, and review where the cluster configuration yaml files are located.
- When using ssh, ensure that you 'exit' from the node to the 'central node.'

The Linux Foundation is strict on the exam requirements and calls for an empty room, no visible writing materials, and a clean desk. Make sure to get a good night's sleep, drink some water beforehand, take 30 minutes before the test to get up, walk around, and take a few deep breaths.

During the Exam

The exam lasts for two hours, although there will be about 15 minutes of setup with the proctor before the exam starts. Once the exam starts, take your time in the first couple of minutes to get settled with the test format. You are allowed two open windows, one for the exam and the other for using external pages. Aim to complete questions in 5 minutes on average since there are approximately 15 questions and 120 mins to complete the exam. This will give you some time for review at the end of the test for review

The CKS, and Kubernetes exams in general, reward precision and time control. Rushing through the questions may give you more time for review, however, a misconfiguration or typo in the YAML files could lead to a loss of all points on a problem. It is better to be efficient the first time than to switch contexts multiple times. Lastly, if you have no idea what the question is asking, we recommend moving onto the next question. It is better to get a couple of questions answered correctly at the beginning than wasting time on unknowns.

Now that you understand the expectations let's walk through the core exam concepts and topics.

Section 1: Cluster Setup

The first section focuses on controlling access to the Kubernetes cluster. The Linux Foundation course outline highlights the following core concepts.

1. Use Network Policies to restrict cluster level access
2. Use the CIS Kubernetes Benchmark to review the security configuration of Kubernetes components (etcd, kubelet, kube-dns, kube-api)
3. Properly set up Ingress objects with security control
4. Protect node metadata and endpoints
5. Minimize use of, and access to, GUI elements
4. Verify platform binaries before deploying

This section takes up 10% of the point total, it is reasonable to assume 2 or 3 questions revolving around cluster setup.

Use Network Policies to restrict cluster level access

Network access between Kubernetes pods is open internally by default. A significant security risk associated with this setup is a container being able to access and connect to other workloads within the cluster network. Network Policies are the answer to this core vulnerability, which means Network Policies will, without a doubt, be in the exam.

Network Policies got an update in version 1.19, so it is worth reviewing the functionality and YAML structure changes. Also, make sure to bookmark these resources as they will come in handy for reference during the exam. If you'd like to learn more about Network Policies, Calico has some great demos, and our own Viswajith Venugopal has provided an extensive writeup of ingress and egress network policies. Lastly, our GitHub repo has multiple questions focused on default-deny policies and setting up ingress objects.

Use the CIS Kubernetes Benchmark to review the security configuration of Kubernetes components (etcd, kubelet, kube-dns, kube-api)

This topic is challenging to narrow down into specific questions. It requires knowledge of the CIS benchmarks that cover version 1.16 to 1.18. kube-bench is an open-source tool that runs validation of the Kubernetes components using the CIS benchmarks. It is worth knowing before the test; however, a question about kube-bench should not be on the test since the webpage is not a listed resource that can be used during the test. With the exam being created with Kubeadm, there may be questions focusing on fixing the core component config files such as kube-apiserver. Knowing how to configure and secure the Kubernetes components is vital to use functionality such as admission controllers, RBAC and avoid a setup where --anonymous-auth was set to true.

Properly set up Ingress objects with security control

Kubernetes Ingress is another concept that will be in the test. Questions could include adding TLS to a previous ingress object or setting up an IngressClass. IngressClass was introduced in version 1.18 and helped to specify how different controllers should implement ingress objects. There are three types of Ingress controller setups to be aware of:

- Cluster-wide Ingress Controller (default)
- Single-namespace Ingress Controller
- Ingress Controller for Specific Ingress Class

Make sure to understand how to implement TLS in Ingress objects and setting up Ingress objects and IngressClass objects.

Protect node metadata endpoints

The topic says it all here. Protecting node metadata and endpoints is always a top concern. In previous Kubernetes versions, the kubelet had a read-only port, port 10255, that could be exploited to learn more about the pods running on the worker nodes. There could be a question where you have to reconfigure kubelet and disable the read-only port. However, the read-only capability has been deprecated, so it seems unlikely this would come up. It is worth knowing all of the endpoints that are required for the Kubernetes cluster to function.

Another use case might be a simple service check. There may be multiple services set up in the exam cluster, and then it is up to the student to weed out any unnecessary services and remove it. It will be worth brushing up on kubectl filtering capabilities and searching by spec.

Minimize use of, and access to, GUI elements

Similar to the previous concept, minimizing access to graphic user interface (GUI) elements is a significant security concern. This topic is fueled by previous security hacks that exposed the Kubernetes Dashboard to the public. To combat this issue, admins should set up internal-only facing dashboards with specific user access outlined in their configuration files.

There may be a question on the exam that requires changing NodePort services or proxying to a dashboard. Another option could be minimizing the permissions of a Dashboard within the cluster. Regardless, making sure that GUI elements are secure should always be a top priority during cluster setup.

Verify platform binaries before deploying

Kubernetes binaries can be verified by referencing their specific checksum in GitHub. Since exam takers will have access to the Kubernetes GitHub repository, it is worth bookmarking the release section and understanding how to verify binary SHA256 hashes.

Section 2: Cluster Hardening

The second section focuses on controlling access to the Kubernetes Cluster environment. The Linux Foundation highlights the following core concepts in their course outline.

1. Restrict access to Kubernetes API
2. Use Role-Based Access Control (RBAC) to minimize exposure
3. Exercise caution in using service accounts, e.g., disable defaults, minimize permissions on newly created ones
4. Update Kubernetes frequently

Knowing that this section takes up 15% of the total point total, it is reasonable to assume 2 or 3 questions revolving around cluster cardening.

Restrict Access to Kubernetes API

Restricting access to the API server is about three things:

- Authentication
- Authorization
- Admission Control

The Kubernetes documentation outlines these topics well, and they are a recommended place to bookmark for the test. Restricting access to the Kubernetes API server is, and will remain, a pervasive topic that will re-emerge in various concepts throughout the test.

Starting with authentication, the CKS may contain a question on user and service account creation and may include creating user certifications or service accounts for deployments. The bootstrap tokens feature probably won't be utilized due to the limitations of the environment setup.

When it comes to authorization, the CKS will focus on RBAC configuration within the cluster as it is enabled by default today. However, there are other authorization modes to be aware of, including:

- Node authorization
- Attribute-based access control (ABAC)
- Webhooks

With the time limitation, the questions around authorization will most likely focus on implementing RBAC policies and using auth can-i to determine API access.

Lastly, admission control will continuously be in use throughout various CKS exam topics. An admission controller intercepts requests to the Kubernetes API after the request is authenticated and authorized but before the object is saved in the key-value store. In the current version, the default admission controllers can be found here, and we recommend bookmarking and getting to know each controller intimately. A significant amount of this exam will be working with various admission controllers to secure the cluster. They will be highlighted as the study guide moves through the six sections.

Use RBAC to minimize exposure

This section is somewhat of a repeat of the previous concept, except this section focuses exclusively on RBAC. The concepts will include:

- Roles
- ClusterRoles
- RoleBindings
- ClusterRoleBindings

This concept will also highlight the binding of roles to “subjects” such as users, groups, and service accounts. Expect questions focused on binding service accounts and users to specific access within the cluster.

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

This concept expands on the previous one and focuses on the proper implementation of subjects. This includes setting default service accounts with the lowest permissions and removing unnecessary service account permissions and using the auth can-i functionality to assess API access.

Update Kubernetes frequently

The last topic was added during the detailed CKS announcement and is ambiguous about how this will be tested. There may be an upgrade question as the documentation about upgrading with kubeadm has been significantly better in recent releases. For instance, a student must upgrade from version 1.18 to 1.19 or possibly drain and update a single node on the cluster. This topic addition is most likely due to version 1.15 being the average cluster version in production today and, in parallel, the community’s desire to get users to take advantage of the updated security features in the last few releases.

Section 3: System Hardening

The third section of our study guide focuses on minimizing the attack surface in the cluster as well as kernel access. The Linux Foundation highlights the following core concepts in their course outline:

1. Minimize host OS footprint (reduce attack surface)
2. Minimize Identity and Access Management (IAM) roles
3. Minimize external access to the network
4. Appropriately use kernel hardening tools such as AppArmor or seccomp

This section takes up 15% of the total point total, and it is reasonable to assume 3-4 questions revolving around system hardening.

Minimize host OS footprint (reduce attack surface)

Minimizing the surface area of attack on your workloads is always an important task. There are three main aspects of reducing the attack surface of your machines:

- Remove unnecessary packages
- Identify and address open ports
- Shut down any unnecessary services

When applying this to the CKS exam, let's review what is reasonable to expect as questions. It is improbable that a student will have to navigate the Ubuntu OS and remove packages during the exam. Instead, the CKS may ask a student to stop containers running with privileged permissions in the cluster. Also, CronJob and container exploitation are serious threats that the CKS may be trying to highlight.

Network Policies are the default network segmentation tool in Kubernetes. It is unlikely that students will have to use a tool like ufw to secure the host, although do not rule it out. Most likely, students will have to shut down exposed services and set up default deny rules inside Kubernetes namespaces to minimize network access.

The exam may also ask you to use admission controllers to limit what can and cannot be run in the cluster. Security contexts are used for multiple security aspects, such as setting process UIDs and not allowing write access to the container filesystem. Controllers such as SecurityContextDeny are useful tools for limiting the scope of pod processes as well.

Minimize IAM roles

Typically, IAM roles are referenced when talking about cloud providers. Although it is not apparent how this concept will manifest during the exam, students can be sure that minimizing access through role-based access control (RBAC) will be a consistent theme.

Minimize external access to the network

Minimizing external access is a small repetition of the first concept. Students may see the network policy implementation expand to include IP blocks and specific ingress and egress rules. Also, students may be required to investigate PodSecurityPolicies (PSP) that allow access to the host network or other privileges that may give a container elevated access. However, implementing PSPs during the exam is unlikely, considering that the feature will most likely be deprecated in version 1.21.

Appropriately use kernel hardening tools such as AppArmor and seccomp

The documentation for the CKS has changed in the past month, and it now allows students to access AppArmor documentation during the exam. There is no link to seccomp documentation, but seccomp profiles have been a GA feature since 1.19.

There is concern over how these concepts will be implemented during the exam. There is a lot of documentation to sift through, and a question on AppArmor implementation may be a time sink if students are not careful. Most likely, there will be a question where students will implement a pre-configured AppArmor profile on the host or using an annotation.

Section 4: Minimize Microservice Vulnerabilities

The fourth section of our study guide focuses on minimizing microservice vulnerabilities and securing pods at runtime. The Linux Foundation highlights the following core concepts in their course outline.

1. Setup appropriate OS-level security domains using options such as Pod Security Policies (PSP), Open Policy Agent (OPA), and security contexts
2. Manage Kubernetes secrets
3. Use container runtime sandboxes in multi-tenant environments (e.g. gvisor, kata containers)
4. Implement pod-to-pod encryption using mTLS

This section takes up 20% of the total point total, and it is reasonable to assume 3-5 questions revolving around minimizing microservice vulnerabilities.

Setup appropriate OS-level security domains using options such as Pod Security Policies (PSP), Open Policy Agent (OPA), and security contexts

Overall this section is the most vague regarding its concepts and what will be asked during the exam. As I mentioned in the previous blog, Pod Security Policies will be deprecated in Kubernetes version 1.21, and Open Policy Agent documentation is not listed as a resource used during the exam. Security contexts are here to stay, and test-takers should be well-versed in their implementation. While PSPs and OPA are useful to know about, I am unaware of how they will be incorporated into the exam. A question will most likely revolve around implementing a PSP through RBAC controls.

POD Security Policies

Even though PSPs will be deprecated, their functionality within Kubernetes clusters should be known. PSPs are a cluster-level resource that controls a wide variety of aspects from Linux capabilities to UIDs. Unfortunately, one criticism is their confusing application through role-based access control (RBAC) and subtle loopholes that can be exploited. PSPs are applied to the user and any pods they create, which means you need to be familiar with cluster-level roles to users, groups, and service accounts. Students must also be aware of the various controls under the PSP and utilize the `auth can-i` functionality to help debug any authorization issues.

Open Policy Agent

OPA has been integrated into the Kubernetes admission controller framework since version 3.0. The documentation is scant, so assume that if there is a question about it, it will be pulled directly from the blogs on kubernetes.io.

Security Context

Security context refers to the pod.spec and the permissions associated with each pod. Contexts can be set at the pod and container level, and a question focused on debugging and identifying escalating privileges is a simple example that may be used. Overall, any questions around security contexts are going to tie into topics such as seccomp and AppArmor from the previous section and other privilege and access control settings.

Manage Kubernetes secrets

If you are taking the CKS, it means you have passed the CKA. You have already had to deal with secrets management from the first exam, so look for expanding that core concept here. Examples that focus on service account tokens or bootstrap token secrets seem like the next steps. As mentioned in this section, you can also guarantee that TLS secrets overlap with other core security concepts. Overall, focus on knowing how to implement secrets securely and ensure that other containers cannot access the secrets.

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

It is essential to understand container runtime sandboxes and their use cases. There may be a question in the exam asking you to implement a sandbox using the `runtimeClassName:` spec. The exam would have to provide you with gvisor or kata containers enabled in the cluster. The main issue is the lack of documentation from the list of sources you can reference during the exam.

Implement pod-to-pod encryption using mTLS

mTLS is a core concept to securing pod-to-pod communications. Although there may be an example that combines secrets, ingress, and mTLS into a single large question. I doubt that the exam will ask you to create the certificates. However, it is worth bookmarking certificate signing requests and understanding how to implement kubeconfig access and mTLS authentication credentials.

Section 5: Supply Chain Security

The fifth section of our study guide focuses on supply chain security. The Linux Foundation highlights the following core concepts in its course outline.

1. Minimize base image footprint
2. Secure your supply chain: whitelist allowed registries, sign and validate images
3. Use static analysis of user workloads (e.g. Kubernetes resources, Dockerfiles)
4. Scan images for known vulnerabilities

This section takes up 20% of the overall point total, and it is reasonable to assume 3-5 questions revolving around supply chain security.

Minimize base image footprint

Regardless of how this is implemented in the test, minimizing your base images is always a good idea to decrease your containers' attack surface. Always make sure only to include the packages that are necessary for each containerized application. When choosing a base image, note how well maintained the image is and its default installed software. In the exam, I expect you will have the option of selecting from a range of base images and choosing their defaults. There may be a question requiring Trivy to view CVEs related to a base image and then prioritize image selection accordingly. As a core concept, image scanning and minimizing your images is a handy way to lower your cluster's attack surface.

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

Securing the images that are allowed to run in your cluster is essential. Also, you will need to verify that the pulled image is from the correct source. The ImagePolicyWebhook admission controller will allow you to set up rules around what images should be allowed within the cluster. An example rule the admission controller could monitor is not allowing any image with the tag `latest`. You will most likely have to connect the ImagePolicyWebhook with a previously setup webhook server during the exam.

Use static analysis of user workloads (e.g. Kubernetes resources, Dockerfiles)

Static analysis might be the most straightforward concept outline in this course. You will need to vet the configuration of Kubernetes YAML files and Dockerfiles and fix any security issues. This includes setting secure base images, removing unnecessary packages, stopping containers from using elevated privileges, and removing the ability to ssh into a container. When hardening Kubernetes resources, look for elevated privileges, security contexts that allow for a UID of 0, and host volumes that should not be mounted.

Scan images for known vulnerabilities

I mentioned container scanning in the previous section, and it would seem there is some crossover between these two topics. Out of the open-source tools that are allowed, Trivy is the only one focused on container scanning. You are also allowed to use the GitHub documentation during the exam, so it's worth bookmarking the quick start documentation.

Section 6: Monitoring, Logging, and Runtime Security

Our study guide's sixth and final section focuses on monitoring, logging, and runtime security within the cluster. The Linux Foundation highlights the following core concepts in its course outline.

1. Perform behavioral analytics on syscall process and file activities at the host and container level to detect malicious activities
2. Detect threats within a physical infrastructure, apps, networks, data, users, and workloads
3. Detect all phases of attack regardless of where it occurs and how it spreads
4. Perform deep analytical investigation and identification of bad actors within the environment
5. Ensure immutability of containers at runtime
6. Use audit logging to monitor access

This section takes up 20% of the point total, and it is reasonable to assume 3-5 questions revolving around monitoring, logging, and runtime security.

Perform behavioral analytics on syscall process and file activities at the host and container level to detect malicious activities

To perform behavioral analysis of syscall and file activities, you will need to implement a tool to detect threats. Falco is a CNCF incubating project listed in the course documentation as a resource available during the exam. I assume that you will have to use Falco to detect some malicious activity and output it to a file, similar to questions from the CKA.

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

This concept generalizes a lot of previous topics that we have covered in past blogs. Assuming that each of the questions takes an average of 5-6 minutes, it is doubtful the exam will have complicated problems that cannot be solved relatively quickly. One possibility might require you to fully assess a deployment in the cluster and write any vulnerabilities that are found in a file. The exam seeks to determine your knowledge of Kubernetes security threats and how to mitigate them. This concept seems overly broad to narrow down any specific topic.

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

Another somewhat broad concept, however, does highlight various methods of exploitation. Mounted volumes, downloading packages, or using malicious running containers on the host show a significant attack surface that you need to be aware of. There is an excellent blog series focused on the MITRE ATT&CK Framework, which is a great resource for reviewing relevant threats for various attack phases.

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

This is another vague concept that encompasses a variety of techniques and topics that have been covered in previous blogs. Anticipate questions that give you actionable information that you will have to correct. These questions may call for you to change config files, remove any misconfigurations, or protect secrets. Audit logging will help to identify bad actors and changes in Kubernetes environments as well.

Ensure immutability of containers at runtime

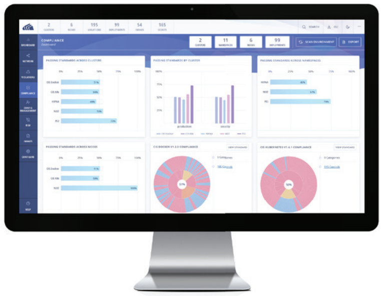
The principle of container immutability means that the containers you have deployed are never changed once they are running - only their images are updated. You want to ensure that the cluster's containers do not execute malicious code added through a download or mounted volume. Students should also be aware of the sidecar pattern and how a volume can be mounted to both containers simultaneously.

Use audit logging to monitor access

Audit logging will make up a significant amount of this section points. The audit policy feature in Kubernetes is another admission controller that allows users to specify what events should be recorded and what data is included. You will most likely need to set up an audit policy during the exam. This question may also tie into identifying bad actors as an audit policy is a helpful way to discover users who are making malicious or unqualified requests in the cluster. Lastly, the log backend might be utilized to output the audit logs to a specific file location.

About StackRox

The StackRox Kubernetes Security Platform is the industry's first and only Kubernetes-native container security platform. It enables security and DevOps teams to work together to protect containerized applications from build to runtime. It integrates with security and DevOps toolchains to help teams operationalize container security. Organizations of all sizes, including cloud-native startups, large enterprises, and government agencies, rely on StackRox to protect their most innovative applications. For more information, visit www.stackrox.com.



Ready to see StackRox in action?

Get a personalized demo tailored for your business, environment, and needs.

REQUEST DEMO