

Kubernetes Sécurité (LFS460) - Certification CKS

Durée: 4 Jours **Réf de cours: SFI-LFS460**

Résumé:

Découvrez les meilleures pratiques de sécurité pour les applications basées sur des conteneurs et les plateformes Kubernetes.

La formation SFI-LFS460 (Kubernetes Security Fundamentals) est le cours officiel Linux Foundation qui vous enseigne les principes et pratiques de sécurisation des clusters Kubernetes.

Ce cours fournit les compétences et les connaissances nécessaires pour maintenir la sécurité dans des environnements dynamiques et multi-projets et pour aborder les problèmes de sécurité des environnements de production cloud.

Grâce à des exercices pratiques, vous apprendrez différentes pratiques de sécurité pour les applications basées sur des conteneurs et les plateformes Kubernetes.

La formation LFS460 couvre l'ensemble du cycle de vie de la sécurité Kubernetes : sécurité de la chaîne d'approvisionnement des images, durcissement du noyau, sécurisation du kube-apiserver, configuration RBAC, Pod Security Admission, protection etcd, politiques réseau, chiffrement pod-à-pod, analyse statique et runtime des charges de travail, contrôle d'accès obligatoire (SELinux, AppArmor), détection d'intrusion, et conformité aux benchmarks CIS. Elle couvre aussi la surveillance continue et la journalisation des événements de sécurité. Ce cours est également conçu pour vous préparer à l'examen de certification Certified Kubernetes Security Specialist (CKS).

Mis à jour 8/6/2026

Public visé:

Toute personne détenant une certification CKA, toute personne intéressée ou responsable de la sécurité cloud.

Objectifs pédagogiques:

- A l'issue de la formation, les participants seront capables de :
- Apprendre à maintenir la sécurité dans des environnements dynamiques et multi-projets
- Aborder les problèmes de sécurité pour les environnements de production cloud
- Utiliser des laboratoires pratiques pour apprendre les meilleures pratiques de sécurité pour les applications basées sur des conteneurs et les plateformes Kubernetes
- Acquérir les connaissances et compétences clés relatives à l'examen de certification Certified Kubernetes Security Specialist (CKS)

Pré-requis:

- Une expérience pratique de 6 mois minimum sur des clusters Kubernetes en production est fortement recommandée
- Une bonne compréhension de Linux
- Familiarité avec la ligne de commande
- Familiarité avec les gestionnaires de paquets
- Familiarité avec Git et GitHub
- Maîtrise de l'utilisation de Kubernetes (l'équivalent d'une certification CKA)
- Connaissances en sécurité Linux (permissions, SELinux/AppArmor) et en réseau (TCP/IP, firewalls)

Test et certification

Ce cours prépare à l'examen de certification Certified Kubernetes Security Specialist (CKS). Cette certification CKS (Certified Kubernetes Security Specialist) est l'examen pratique le plus avancé de l'écosystème Kubernetes, validant votre capacité à sécuriser des environnements de production.

Prévoyez 4 à 6 semaines de pratique intensive après la formation. L'examen dure 2 heures avec des scénarios complexes nécessitant rapidité et précision.

La certification CKA (Certified Kubernetes Administrator) est un prérequis obligatoire pour passer la certification CKS. Vous devez détenir un CKA valide au moment de l'inscription à l'examen CKS.

NB: L'examen n'est pas inclus dans le prix de la formation.

Après cette formation, nous vous conseillons le(s) module(s) suivant(s):

Pas de recommandation.

Contenu:

1.Introduction

- Les certifications de la Linux Foundation
- Les badges numériques de la Linux Foundation
- Exercices de laboratoire, solutions et ressources
- Les choses qui changent dans Linux et les projets Open Source
- Cours en ligne : LFS260
- Détails de la plateforme

2.Aperçu de la Sécurité Cloud

- Projets multiples
- Qu'est-ce que la sécurité ?
- Évaluation
- Prévention
- Détection
- Réaction
- Catégories d'attaquants
- Types d'attaques
- Surfaces d'attaque
- Considérations sur le matériel et le micrologiciel
- Agences de sécurité
- Gérer l'accès externe
- Laboratoires

3.Préparation à l'Installation

- Chaîne d'approvisionnement des images
- Sandbox d'exécution
- Vérifier les binaires de la plateforme
- Minimiser l'accès à l'interface graphique
- Contrôle basé sur des politiques
- Laboratoires

4.Installation du Cluster

- Mettre à jour Kubernetes
- Outils pour durcir le noyau
- Exemples de durcissement du noyau
- Atténuation des vulnérabilités du noyau
- Laboratoires

5.Sécurisation du kube-apiserver

- Restreindre l'accès à l'API
- Activer l'audit du Kube-apiserver
- Configuration de RBAC
- Admission de sécurité des pods
- Minimiser les rôles I
- Protéger etcd
- Benchmark CIS
- Utilisation des comptes de service
- Laboratoires

6.Réseau

- Bases du pare-feu
- Plugins réseau
- Atténuer les tentatives de connexion par force brute
- Objets Ingress
- Chiffrement de pod à pod
- Restreindre l'accès au niveau du cluster
- Laboratoires

7.Considérations sur les Charges de Travail

- Minimiser l'image de base
- Analyse statique des charges de travail
- Analyse d'exécution des charges de travail
- Aperçu de SBOM
- Immuabilité des conteneurs
- Contrôle d'accès obligatoire
- SELinux
- AppArmor
- Générer des profils AppArmor
- Laboratoire

8. Détection des Problèmes

- Comprendre les phases d'une attaque
- Préparation
- Comprendre la progression d'une attaque
- Pendant un incident
- Gestion des suites d'un incident
- Systèmes de détection d'intrusion
- Détection des menaces
- Analyse comportementale
- Laboratoire

9. Révision des Domaines

- Préparation à l'examen
- Laboratoires

10. Clôture et Enquête d'Évaluation

- Enquête d'évaluation

Méthodes pédagogiques :

Un support de cours officiel sera remis aux participants

Autres moyens pédagogiques et de suivi:

- Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
- Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
- En fin de formation, le participant est invité à s'auto-évaluer sur l'atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :

- Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
- Votre place sera confirmée à la réception d'un devis ou "booking form" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
- Attention, si cette formation est éligible au Compte Personnel de Formation, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés avant le début de la session pour vous inscrire via moncompteformation.gouv.fr.

Accueil des bénéficiaires :

- En cas de handicap : plus d'info sur globalknowledge.fr/handicap
- Le Règlement intérieur est disponible sur globalknowledge.fr/reglement