

## Sécuriser les clusters Kubernetes avec Red Hat Advanced Cluster Security(DO430)

Durée: 3 Jours    Réf de cours: DO430    Méthodes d'apprentissage: Intra-entreprise & sur-mesure

### Résumé:

#### Résoudre les problèmes de sécurité avec Red Hat Advanced Cluster Security for Kubernetes dans un environnement de cluster OpenShift.

Les clients souhaitent savoir comment la solution Red Hat Advanced Cluster Security for Kubernetes (RHACS) peut les aider à relever leurs défis en matière de sécurité. Cependant, il se peut que leurs équipes de sécurité n'aient pas suffisamment d'expérience avec Kubernetes et OpenShift, ce qui pose des problèmes lors de la mise en œuvre.

Ces équipes ont notamment les besoins suivants :

- Intégration de la solution RHACS aux pratiques DevOps et maîtrise de son utilisation pour automatiser le modèle DevSecOps, afin de permettre aux équipes de mettre en œuvre et sécuriser la chaîne logistique, l'infrastructure et les charges de travail
- Évaluation de conformité d'après les normes du secteur et obtention de conseils sur la correction des problèmes
- Gestion des vulnérabilités, application des politiques et segmentation du réseau pour sécuriser les charges de travail

Certains clients RHACS utilisent déjà des registres d'images externes ainsi que des outils de gestion des informations et des événements de sécurité. Pour atteindre leurs objectifs en matière de sécurité, ils doivent intégrer la solution RHACS à leurs composants externes.

Le cours Sécuriser les clusters Kubernetes avec Red Hat Advanced Cluster **Security** s'adresse aux clients qui exécutent des charges de travail conteneurisées sur Kubernetes et qui sont souvent confrontés à plusieurs problèmes liés à la sécurité.

Il explique comment la solution RHACS propose des solutions pratiques pour relever ces défis, aider les équipes à sécuriser les environnements Kubernetes plus efficacement et rationaliser les workflows de développement afin d'inclure des contrôles de sécurité dès le départ.

**Remarque :** La souscription RHLS-Course remplace l'inscription à une formation en distanciel

À compter du 1er janvier 2026, Red Hat lance RHLS-Course, un modèle de souscription flexible. Lorsque vous achetez cette souscription, cela vous donne la liberté de choisir la session qui vous convient le mieux et de vous inscrire vous-même à la date de votre choix.

La souscription RHLS-Course comprend :

- Un droit d'accès à une session distanciel animée par un formateur
- 12 mois d'accès à l'apprentissage à votre rythme
- Un examen de certification avec 2eme essai inclus

Les modalités des sessions en classe présentielle sur site et les sessions dédiées intra-entreprise restent inchangées.

Mis à jour 19/01/2026

Formation intra-entreprise

Cette formation est délivrable en session intra-entreprise, dans vos locaux ou dans les nôtres. Son contenu peut être adapté sur-mesure pour répondre aux besoins de vos collaborateurs. Contactez votre conseiller formation Global Knowledge ou adressez votre demande à [info@globalknowledge.fr](mailto:info@globalknowledge.fr).

### Public visé:

Professionnels de la sécurité responsables de l'identification, de l'analyse et de l'atténuation des menaces de sécurité dans les environnements Kubernetes Administrateurs d'infrastructure chargés de gérer et sécuriser les clusters Kubernetes, et de veiller à ce que l'infrastructure soit robuste et conforme aux normes de sécurité Ingénieurs de plateformes qui suivent les pratiques DevOps et DevSecOps et qui intègrent la sécurité au pipeline CI/CD pour sécuriser le déploiement et la surveillance continue des applications conteneurisées

### Objectifs pédagogiques:

- A l'issue de la formation, les participants seront capables de :
- Décrire et mettre en œuvre l'architecture RHACS et de ses composants, suivi des pratiques recommandées pour son installation et résolution des problèmes d'installation courants
- Interpréter des résultats d'analyse des vulnérabilités, génération de rapports de vulnérabilité et évaluation des risques afin de hiérarchiser les actions de sécurité
- Mettre en œuvre et appliquer des politiques RHACS à toutes les étapes impliquant l'application de politiques pour sécuriser le pipeline CI/CD et protéger la chaîne d'approvisionnement des logiciels
- Identifier et résoudre des failles de sécurité dans les politiques réseau à l'aide de Network Graph et application des politiques réseau générées dans un pipeline CI/CD
- Exécuter des analyses de conformité intégrées, installer et exécuter l'opérateur de conformité pour déterminer la conformité du cluster avec les politiques et les normes de sécurité, et production de rapports et de preuves de conformité
- Intégrer RHACS à des composants externes afin de profiter de fonctions supplémentaires, dont la notification d'alertes centralisée, la sauvegarde et la restauration, ainsi que la gestion des identités et des autorisations

---

## Pré-requis:

- Avoir suivi le cours Administration de Red Hat OpenShift II : configuration d'un cluster de production (DO280)  
Il est vivement recommandé de passer l'évaluation gratuite pour s'assurer que le cours est adapté aux compétences du participant

### [Red Hat Skills Assessment](#)

- DO280 - Red Hat OpenShift Administration II : configuration d'un cluster de production (DO280)

## Test et certification

- Examen Spécialiste certifié Red Hat en utilisation d'OpenShift Advanced Cluster Security (EX430)

---

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

- Red Hat Advanced Cluster Management for Kubernetes (DO432)

---

## Contenu:

### Installation de Red Hat Advanced Cluster Security for Kubernetes

- Décrire et mettre en œuvre l'architecture RHACS et ses composants, suivre les pratiques recommandées pour son installation et résoudre les problèmes d'installation courants

### Gestion des vulnérabilités avec Red Hat Advanced Cluster Security for Kubernetes

- Interpréter des résultats d'analyse des vulnérabilités, générer des rapports de vulnérabilité et évaluer les risques afin de hiérarchiser les actions de sécurité

### Gestion des politiques avec Red Hat Advanced Cluster Security for Kubernetes

- Mettre en œuvre et appliquer des politiques RHACS à toutes les étapes impliquant l'application de politiques pour sécuriser le pipeline CI/CD et protéger la chaîne d'approvisionnement des logiciels

### Segmentation du réseau avec Red Hat Advanced Cluster Security for Kubernetes

- Identifier et résoudre les failles de sécurité dans les politiques réseau à l'aide de Network Graph et appliquer des politiques réseau générées dans un pipeline CI/CD

### Gestion de la conformité avec les normes du secteur avec Red Hat Advanced Cluster Security for Kubernetes

- Exécuter des analyses de conformité intégrées, installer et exécuter l'opérateur de conformité pour déterminer la conformité du cluster avec les politiques et les normes de sécurité, et produire des rapports et des preuves de conformité

### Intégration de composants externes avec Red Hat Advanced Cluster Security for Kubernetes

- Intégrer RHACS à des composants externes afin de profiter de fonctions supplémentaires, dont la notification d'alertes centralisée, la sauvegarde et la restauration, ainsi que la gestion des identités et des autorisations

---

## Méthodes pédagogiques :

Un support de cours officiel sera fourni 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](http://moncompteformation.gouv.fr).

### Accueil des bénéficiaires :

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