

Securing Kubernetes Clusters with Red Hat Advanced Cluster Security (DO430)

Duración: 3 Días **Código del Curso: DO430** **Método de Impartición: Curso Remoto (Virtual)**

Temario:

Address security challenges by applying Red Hat Advanced Cluster Security for Kubernetes in an OpenShift cluster environment.

Customers want to learn how Red Hat Advanced Cluster Security for Kubernetes (RHACS) can help them solve their security challenges. However, their security teams might lack experience with Kubernetes and OpenShift, and so they have challenges with implementation. In particular, their security teams have several needs:

- Integrate RHACS with DevOps practices and know how to use it to automate DevSecOps, to enable their teams to operationalize and secure their supply chain, infrastructure, and workloads
- Assess compliance based on industry-standard benchmarks and get remediation guidance
- Apply vulnerability management, policy enforcement, and network segmentation to secure their workloads

RHACS customers might already be using external image registries and Security Information and Event Management (SIEM) tools. They need to integrate RHACS with their existing set of external components to achieve their security goals.

Note: Starting January 1, 2026, Red Hat introduces RHLS-Course — a flexible subscription model now included with this catalog offering. This replaces the previous direct virtual class enrollment from Global Knowledge.

When you purchase this item, you'll receive an RHLS subscription at the course level, giving you the freedom to choose the schedule that works best and self-enroll in your selected class.

Your RHLS subscription includes:

- One live, instructor-led virtual session
- 12 months of self-paced learning access
- One certification exam with a free retake

Onsite Classroom-based sessions and closed course options remain unchanged.

Updated Jan2026

Virtual Learning

This interactive training can be taken from any location, your office or home and is delivered by a trainer. This training does not have any delegates in the class with the instructor, since all delegates are virtually connected. Virtual delegates do not travel to this course, Global Knowledge will send you all the information needed before the start of the course and you can test the logins.

Dirigido a:

Security practitioners who are responsible for identifying, analyzing, and mitigating security threats within Kubernetes environments
Infrastructure administrators who are tasked with managing and securing Kubernetes clusters and ensuring that the infrastructure is robust and compliant with security standards
Platform engineers who follow DevOps and DevSecOps practices, who integrate security into the CI/CD pipeline, to ensure the secure deployment and continuous monitoring of containerized applications

Objetivos:

- After this course participants should be able to:
 - Identify and close security gaps in network policies by using Network Graph and apply the generated network policies in a CI/CD pipeline
- Describe and implement the RHACS architecture and its components, follow recommended practices for its installation, and troubleshoot common installation issues
 - Run in-built compliance scans, and install and run the compliance operator to determine cluster compliance with security policies and standards and to produce reports and evidence of compliance
- Interpret vulnerability scanning results, generate vulnerability reports, and evaluate risks to prioritize your security actions
 - Integrate RHACS with external components to provide additional functions, which include centralized alert notification, backup and restore, and identity and permission management
- Implement and enforce RHACS policies across all stages of policy enforcement to secure the CI/CD pipeline and to protect the software supply chain

Prerequisites:

- Red Hat OpenShift Administration II: Configuring a Production Cluster | DO280 is a prerequisite or equivalent knowledge

Exámenes y certificación

- Red Hat Certified Specialist in OpenShift Advanced Cluster Security Exam (EX430)

Take Red Hat free assessment to gauge whether this offering is the best fit for your skills [Red Hat Skills Assessment](#)

- DO280 - Red Hat OpenShift Administration II: Configuring a Production Cluster

Siguientes cursos recomendados:

- Red Hat Advanced Cluster Management for Kubernetes Classroom Training (DO432)

Contenido:

Installing Red Hat Advanced Cluster Security for Kubernetes

- Describe and implement the RHACS architecture and its components, follow recommended practices for its installation, and troubleshoot common installation issues.

Vulnerability Management with Red Hat Advanced Cluster Security for Kubernetes

- Interpret vulnerability scanning results, generate vulnerability reports, and evaluate risks to prioritize your security actions.

Policy Management with Red Hat Advanced Cluster Security for Kubernetes

- Implement and enforce RHACS policies across all stages of policy enforcement to secure the CI/CD pipeline and to protect the software supply chain.

Network Segmentation with Red Hat Advanced Cluster Security for Kubernetes

- Identify and close security gaps in network policies by using Network Graph and apply the generated network policies in a CI/CD pipeline.

Manage Compliance with Industry Standards with Red Hat Advanced Cluster Security for Kubernetes

- Run in-built compliance scans, and install and run the compliance operator to determine cluster compliance with security policies and standards and to produce reports and evidence of compliance.

Integrate External Components with Red Hat Advanced Cluster Security for Kubernetes

- Integrate RHACS with external components to provide additional functions, which include centralized alert notification, backup and restore, and identity and permission management.

Información Adicional:

Official course book provided to participants

Más información:

Para más información o para reservar tu plaza llámanos al (34) 91 425 06 60

info.cursos@globalknowledge.es

www.globalknowledge.com/es-es/

Global Knowledge Network Spain, C/ Retama 7, 6ª planta, 28045 Madrid