DO431

Securing Kubernetes Clusters with Red Hat Advanced Cluster Security with Exam

Course Description

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.

This course is based on Red Hat Advanced Cluster Security 4.6. The Red Hat Certified Specialist in OpenShift Advanced Cluster Security Exam (EX430) is included in this offering.

Prerequisites for this course

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

Course Outline

Outline for this course

1. **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.

2. **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.

3. **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.

4. **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.

5. **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.

6. **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**.**