DO430
Securing Kubernetes Clusters with Red Hat Advanced Cluster Security

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.

Course content summary

- Describe and implement the RHACS architecture and its components, follow recommended practices for its installation, and troubleshoot common installation issues
- Interpret vulnerability scanning results, generate vulnerability reports, and evaluate risks to prioritize your security actions
- Implement and enforce RHACS policies across all stages of policy enforcement to secure the CI/CD pipeline and to protect the software supply chain
- Identify and close security gaps in network policies by using Network Graph and apply the generated network policies in a CI/CD pipeline
- 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 RHACS with external components to provide additional functions, which include centralized alert notification, backup and restore, and identity and permission management

Course reference: https://www.redhat.com/en/services/training/do430-securing-kubernetes-clusters-red-hat-advanced-cluster-security

Audience for this course

- 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

Prerequisites for this course

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

Outline for this course

- **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.

Impact on the individual

As a result of attending this course, students will be able to install and use RHACS and to secure their Kubernetes workloads and clusters according to the best industry practice.

Students should be able to demonstrate the following skills:

Course reference: https://www.redhat.com/en/services/training/do430-securing-kubernetes-clusters-red-hat-advanced-cluster-security

- Installing RHACS Central and importing secure clusters
- Troubleshooting and fixing common installation issues
- Interpreting vulnerability results and generating reports
- Identifying and mitigating risks in deployments
- Creating and enforcing build, deployment, and runtime policies
- Implementing policy checks in a CI/CD pipeline to secure the software supply chain
- Applying network segmentation to reduce attacks
- Generating and applying network policies within a CI/CD pipeline by using roxctl commands
- Managing and retrieving compliance evidence
- Applying third-party integrations for centralized alert notification, backup and restore, and identity and permission management

Course reference: https://www.redhat.com/en/services/training/do430-securing-kubernetes-clusters-red-hat-advanced-cluster-security