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

ID DO430 **Price** CHF 2,805.—(excl. VAT) **Duration** 3 days

Who should attend

- 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

Red Hat OpenShift Administration II: Configuring a Production Cluster (DO280)

Course Objectives

Impact on the Organization

Securing Kubernetes Clusters with Red Hat Advanced Cluster Security supports customers who run containerized workloads on Kubernetes, and who often face several security-related challenges:

- Delays in container deployments due to security issues
- Revenue loss due to Kubernetes-related security incidents
- Decreased developer productivity due to time that is spent to address security concerns

This course teaches how RHACS provides actionable solutions to address these challenges, to help teams secure their Kubernetes environments more effectively and to streamline development workflows to include security checks at an early stage.

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:

- 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 Content

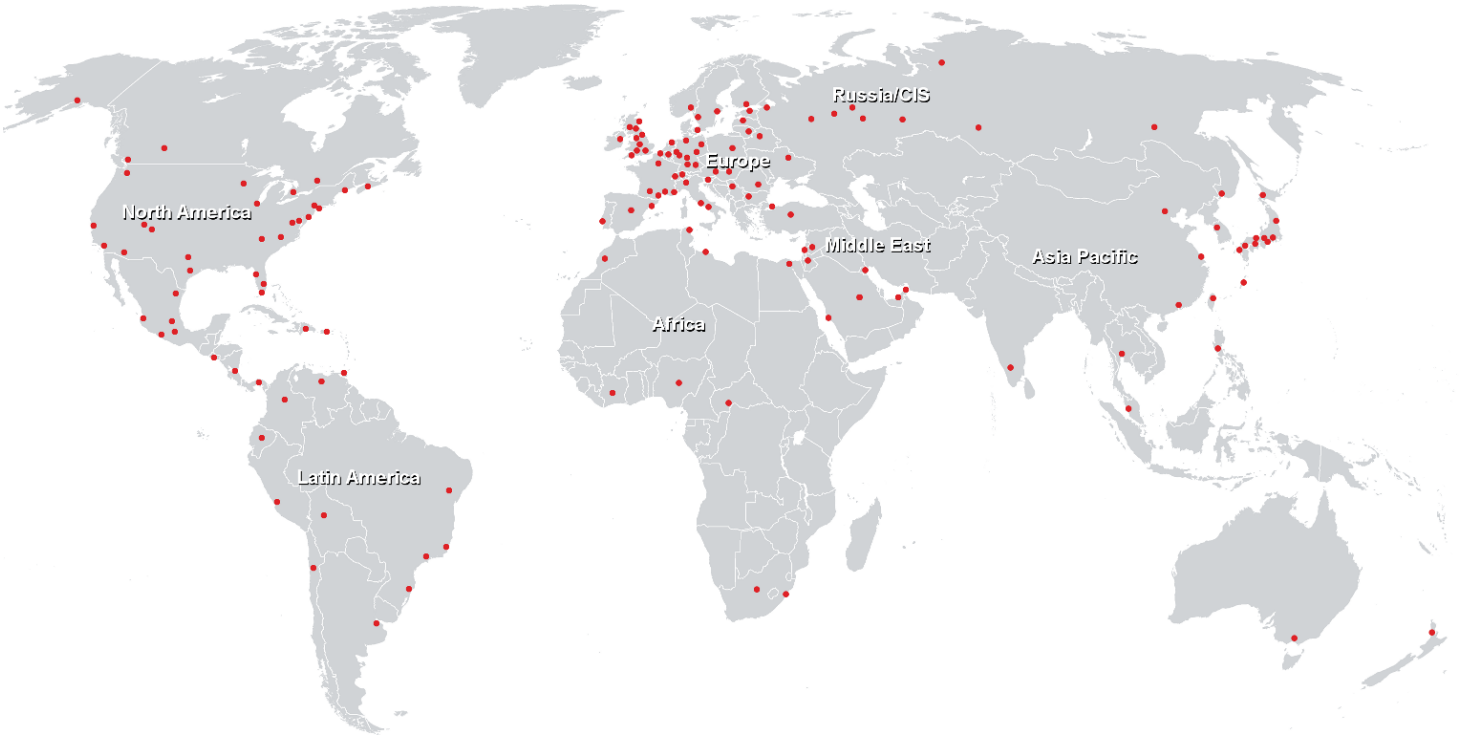
Course Content Summary

- 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

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

Training Centres worldwide





Fast Lane Institute for Knowledge Transfer (Switzerland) AG

Husacherstrasse 3
CH-8304 Wallisellen
Tel. +41 44 832 50 80

info@flane.ch, https://www.flane.ch