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

Duration: **3 Day**

BILGINC IT Academy
info@bilginc.com
bilginc.com

Overview

Securing Kubernetes Clusters with Red Hat Advanced Cluster Security is an advanced course designed for IT professionals responsible for securing Kubernetes and OpenShift environments using **Red Hat Advanced Cluster Security for Kubernetes (RHACS)** . The programme provides practical guidance for deploying, configuring, and managing RHACS while implementing security controls across containerized application environments.

Throughout the course, participants will learn how to manage vulnerabilities, enforce security policies, implement network segmentation, perform compliance assessments, and integrate RHACS with external enterprise security solutions. The programme focuses on protecting Kubernetes workloads throughout the entire application lifecycle while strengthening DevSecOps practices.

Learners will also explore how RHACS supports secure software supply chains by integrating security into CI/CD pipelines, automating policy enforcement, and helping organizations comply with industry security standards.

By the end of the programme, participants will be able to secure Kubernetes clusters more effectively, prioritize security risks, implement compliance controls, and integrate RHACS into enterprise security ecosystems.

Organizational Benefits

After completing this course, organizations will be able to:

- Improve the security posture of Kubernetes environments.
- Reduce deployment delays caused by security issues.
- Strengthen DevSecOps implementation across development teams.
- Protect the software supply chain through automated security controls.
- Integrate security validation into CI/CD pipelines.
- Increase operational efficiency while improving developer productivity.

Individual Benefits

Upon successful completion of the course, participants will be able to:

- Install RHACS Central and onboard secure Kubernetes clusters.
- Troubleshoot common installation and configuration issues.
- Analyze vulnerability reports and prioritize remediation.
- Assess deployment risks and strengthen workload security.
- Create and enforce build, deployment, and runtime security policies.
- Integrate security controls into CI/CD pipelines.
- Implement network segmentation and manage network policies.
- Generate compliance reports and audit evidence.
- Integrate RHACS with SIEM, identity management, backup, and other enterprise security platforms.

Recommended Next Course or Certification

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

Duration: **3 Day**

BILGINC IT Academy
info@bilginc.com
bilginc.com

Participants wishing to continue their learning journey are encouraged to consider:

- **Red Hat Certified Specialist in OpenShift Advanced Cluster Security (EX430)**
- **Red Hat Advanced Cluster Management for Kubernetes (DO432)**

Prerequisites

Participants are recommended to have:

- A working knowledge of Kubernetes and Red Hat OpenShift administration.
- Experience equivalent to **Red Hat OpenShift Administration II: Configuring a Production Cluster (DO280)**.
- Completion of the Red Hat skills assessment is recommended to evaluate course readiness.

Who Should Attend

This course is designed for:

- Security professionals responsible for protecting Kubernetes environments.
- Infrastructure administrators managing Kubernetes clusters.
- Platform engineers implementing DevOps and DevSecOps practices.
- Engineers responsible for integrating security into CI/CD pipelines.
- System administrators managing containerized application platforms.
- Technical teams responsible for Kubernetes security, governance, and compliance.

What You Will Learn

Upon successful completion of this course, participants will be able to:

- Install and configure Red Hat Advanced Cluster Security and onboard secure Kubernetes clusters.
- Troubleshoot common RHACS deployment and configuration issues.
- Analyze vulnerability assessment results and prioritize remediation activities.
- Create and enforce security policies across build, deployment, and runtime environments.
- Integrate security controls into DevSecOps pipelines to protect the software supply chain.
- Design and implement network segmentation policies for Kubernetes workloads.
- Perform compliance assessments and generate audit evidence using RHACS tools.
- Integrate RHACS with SIEM platforms, identity providers, backup solutions, and other enterprise security services.

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

Duration: **3 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Outline

Module 1 - Installing Red Hat Advanced Cluster Security

- Understanding the RHACS architecture
- Installing and configuring core platform components
- Importing and securing Kubernetes clusters
- Applying recommended installation practices
- Troubleshooting common deployment issues

Module 2 - Vulnerability Management

- Interpreting vulnerability scan results
- Assessing security risks
- Generating vulnerability reports
- Prioritizing remediation activities
- Reducing security exposure across Kubernetes workloads

Module 3 - Policy Management

- Creating and managing RHACS security policies
- Applying policies during build, deployment, and runtime stages
- Automating policy enforcement throughout CI/CD pipelines
- Protecting the software supply chain using DevSecOps practices

Module 4 - Network Segmentation

- Strengthening Kubernetes network security
- Using Network Graph to analyze workload communication
- Identifying network security gaps
- Creating and enforcing network policies
- Automating network policy deployment using roxctl within CI/CD workflows

Module 5 - Compliance Management

- Running built-in compliance scans
- Installing and using the Compliance Operator
- Assessing compliance against security standards
- Generating compliance reports
- Producing audit evidence for regulatory requirements

Module 6 - Integrating External Components

- Integrating RHACS with enterprise security platforms
- Centralized alerting through SIEM solutions
- Managing backup and recovery integrations
- Connecting identity and access management services
- Extending RHACS capabilities through third-party integrations