Building Resilient Microservices with Istio and Red Hat OpenShift Service Mesh (DO328) Training

Duration: **3 Day**

BİLGİNÇ IT Academy
info@bilginc.com
+44 20 3807 0925
+90 212 282 7700

Overview

Control, manage, trace, and secure microservices communications with **Red Hat OpenShift Service Mesh**, powered by **Istio**.

Modern microservice applications can become complex to manage, especially as the number of services and communication pathways grows.
Red Hat OpenShift Service Mesh simplifies this by providing a **unified platform for traffic control, service observability, security, and resilience** across distributed systems.

The {*training} teaches developers and engineers how to implement, monitor, and secure microservices within an **enterprise-grade OpenShift environment**.

> *This course is based on Red Hat OpenShift Service Mesh 3.1 and OpenShift 4.18.*

Prerequisites

- Completion of *Red Hat OpenShift Developer II: Building and Deploying Cloud-native Applications (DO288)* or equivalent OpenShift experience.
- Knowledge of **microservice development** (such as *DO378: Cloud-native Microservices with Quarkus*) is recommended but not mandatory.

Who Should Attend

This course is designed for:

- **Developers** and **platform engineers** responsible for building, managing, and securing microservice communication on **Red Hat OpenShift**.

Building Resilient Microservices with Istio and Red Hat OpenShift Service Mesh (DO328) Training

Duration: **3 Day**

BİLGİNÇ IT Academy
info@bilginc.com
+44 20 3807 0925
+90 212 282 7700

What You Will Learn

By the end of this {*training}, you will have gained knowledge and skills in the following areas:

- **Introducing OpenShift Service Mesh**
  Learn the fundamentals of microservice communication, observability, and security in distributed environments.
- **Observing OpenShift Service Mesh**
  Trace, monitor, and visualize service interactions with OpenShift's observability tools.
- **Managing Traffic**
  Apply routing strategies, resilience policies, and fault-injection techniques to build reliable systems.
- **Securing OpenShift Service Mesh**
  Implement zero-trust principles and secure traffic between services.
- **Comprehensive Review**
  Reinforce your understanding through review and practical exercises.

Impact on the Organization

Organizations adopting **microservices, AI integration, and hybrid architectures** face new operational challenges.
Red Hat OpenShift Service Mesh empowers teams to manage these complex environments by offering:

- Centralized **traffic control** and routing.
- Real-time **observability and tracing**.
- Integrated **security and encryption** for all communications.
- Improved **resilience** through intelligent policies.

By implementing this course's practices, enterprises can**reduce downtime, increase reliability**, and **streamline DevOps operations** in microservice-based systems.

Impact on the Individual

After completing this course, participants will be able to:

- Understand the **architecture and components** of OpenShift Service Mesh.
- **Trace and visualize** application traffic across services.
- Apply **routing rules**, **resiliency techniques**, and **traffic control** policies.
- Design and enforce **zero-trust security** for microservice communications.
- Confidently manage and monitor distributed applications in**OpenShift** environments.

Building Resilient Microservices with Istio and Red Hat OpenShift Service Mesh (DO328) Training

Duration: **3 Day**

BILGINÇ IT Academy
info@bilginc.com
+44 20 3807 0925
+90 212 282 7700

Outline

1. Introducing OpenShift Service Mesh
Understand microservice architecture and how OpenShift Service Mesh enhances visibility, security, and traffic management.

2. Observing the Service Mesh
Use OpenShift observability tools to trace and visualize application traffic flow.

3. Managing Application Traffic
Configure routing, retries, and fault-injection techniques to improve system resilience and reliability.

4. Securing the Service Mesh
Apply **zero-trust security principles** — ensuring all service-to-service communication is encrypted, authenticated, and authorized.

5. Comprehensive Review
Review course concepts and validate practical understanding through guided labs.