Building a Sovereign Cloud with Red Hat OpenShift (DO505) Training

Duration: **5 Day**

BILGINC IT Academy
info@bilginc.com
bilginc.com

Designing and Operating Cloud Platforms for Digital Sovereignty

Building a Sovereign Cloud with Red Hat OpenShift (DO505) provides the skills required to design, build, and operate secure multitenant cloud platforms that meet digital sovereignty requirements by using Red Hat OpenShift.

Designed for enterprise architects, IT security professionals, and operations teams, the course is based on **Red Hat OpenShift Container Platform 4.20**.

Throughout the course, participants explore sovereign cloud design through the principles of the European Union Cloud Sovereignty Framework. Key areas include deploying multitenant clusters-as-a-service with hosted control planes, enforcing jurisdiction-aware access controls, applying zero-trust isolation, and implementing advanced cryptographic protections.

Participants also gain hands-on experience with external key management, network-bound disk encryption, confidential computing, and post-quantum cryptography as part of a broader sovereign cloud security strategy.

Organizational Impact

DO505 helps organizations develop the technical expertise required to operate multitenant cloud platforms while meeting digital sovereignty requirements such as those defined by the EU Cloud Sovereignty Framework.

Knowledge of hosted control plane isolation, jurisdiction-aware identity and access controls, external key management, and cryptographic protection across different data states can help organizations satisfy regulatory expectations related to data residency, personnel sovereignty, and cryptographic control.

This expertise also supports the delivery of sovereign clusters-as-a-service with verifiable jurisdictional guarantees while helping reduce the risk of regulatory noncompliance.

Individual Impact

DO505 provides participants with an advanced, hands-on understanding of how to design and operate sovereign cloud infrastructure on Red Hat OpenShift.

Participants gain practical experience deploying multitenant hosted control planes, implementing zero-trust workload identity with SPIFFE and SPIRE, integrating external key management systems, configuring network-bound disk encryption, and applying jurisdiction-aware access controls.

These skills enable enterprise architects, IT security practitioners, and operations engineers to design and operate cloud platforms that meet demanding digital sovereignty requirements with greater confidence.

Building a Sovereign Cloud with Red Hat OpenShift (DO505) Training

Duration: **5 Day**

BILGINC IT Academy
info@bilginc.com
bilginc.com

Prerequisites

Participants should have or consider the following skills and experience:

- Taking the Red Hat skills assessment is recommended to determine whether the course matches your current skill level
- Completion of **Red Hat OpenShift Administration II: Configuring a Production Cluster (DO280)** or equivalent experience managing and troubleshooting a self-managed OpenShift cluster
- Familiarity with core security concepts such as Identity and Access Management (IAM), encryption, network policies, and firewalls
- Completion of **Multicluster Management with Red Hat Advanced Cluster Management for Kubernetes (DO432)** or equivalent RHACM experience is recommended but not required

Who Should Attend

This course is particularly suitable for:

- Enterprise architects responsible for designing sovereign landing zones, control planes, and integrated sovereignty controls
- IT security practitioners who translate regulatory requirements, including the SOV framework, into technical policies
- Security professionals responsible for cryptographic controls, identity, and access management
- IT operations personnel who implement and manage sovereign controls on a daily basis
- SREs responsible for maintaining operational resilience
- System administrators who operate sovereign cloud controls within Red Hat OpenShift environments

What You Will Learn

The course covers the following key areas:

- Defining the core pillars of digital sovereignty and mapping sovereignty goals to a multicluster OpenShift architecture
- Deploying sovereign edge clusters in air-gapped environments
- Designing multitenant isolation by using hosted control planes
- Enforcing GitOps as the sovereign source of truth for infrastructure management
- Implementing jurisdiction-aware identity and access controls
- Establishing zero-trust workload identity with SPIFFE and SPIRE
- Integrating external key management to support cryptographic sovereignty
- Supporting data residency through network-bound disk encryption and confidential computing
- Preparing for post-quantum cryptography threats
- Implementing sovereign disaster recovery with backups that remain within the required jurisdiction

Building a Sovereign Cloud with Red Hat OpenShift (DO505) Training

Duration: **5 Day**

BILGINC
IT Academy
info@bilginc.com
bilginc.com

Training Outline

1. Introduction to Sovereign Cloud Operations

Explore the four pillars of digital sovereignty and the European Union Sovereignty Objectives (SOV).

Examine the role of the Red Hat Advanced Cluster Management (RHACM) hub-and-spoke architecture within sovereign cloud provider environments and understand how multicluster management supports sovereignty objectives.

2. Architecting the Sovereign Boundary

Learn how to onboard and manage sovereign clusters-as-a-service tenant clusters by using RHACM.

Apply zero-trust isolation, operational sovereignty, and jurisdiction-aware access controls across hosted control plane and multitenant environments.

This section also explores how sovereign boundaries can be enforced across identity, access, operations, and infrastructure layers.

3. Securing Sovereign Data

Implement advanced cryptographic controls for tenant clusters and provider workloads.

Learn how to protect data confidentiality across data at rest, data in use, and recovery scenarios by integrating technologies such as external key management, network-bound disk encryption, and confidential computing.

Participants also explore preparation for post-quantum cryptography threats and the design of disaster recovery processes that keep protected data within the required jurisdiction.