

Building a Sovereign Cloud with Red Hat OpenShift

OEM: Red Hat • Code: DO505



COURSE DESCRIPTION

Design, build, and operate a sovereign cloud platform with multitenant isolation, jurisdiction-aware access controls, and advanced cryptographic protections by using Red Hat OpenShift.

This course is designed for enterprise architects, IT security practitioners, and operations personnel who need to meet digital sovereignty requirements by using Red Hat OpenShift Container Platform 4.20. Grounded in the European Union (EU) Cloud Sovereignty Framework, learners will gain hands-on proficiency in deploying multitenant clusters-as-a-service with hosted control planes, enforcing zero-trust isolation and jurisdiction-aware access controls, and implementing advanced cryptographic protections including external key management, network-bound disk encryption, and post-quantum cryptography.

COURSE CONTENT SUMMARY

- Defining the pillars of digital sovereignty and mapping sovereignty objectives to a multicluster OpenShift architecture.
- Deploying sovereign edge clusters in air-gapped environments.
- Architecting multitenant isolation with 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 for cryptographic sovereignty.
- Securing data residency with network-bound disk encryption and confidential computing.
- Preparing for post-quantum cryptography threats.
- Implementing sovereign disaster recovery with in-jurisdiction backups.

AUDIENCE PROFILE

- Enterprise Architects who design the sovereign landing zone, control planes, and integrate sovereign controls.
- IT Security Practitioners who translate regulatory law (such as the SOV framework) into technical policy and manage cryptographic controls.
- IT Operations personnel, SREs, and System Administrators who implement, manage, and automate sovereign controls daily and ensure operational resilience.

PREREQUISITES

- Red Hat OpenShift Administration II: Configuring a Production Cluster (DO280), or equivalent experience with managing and troubleshooting a self-managed OpenShift cluster.
- Security fundamentals: familiarity with core security concepts, such as identity and access management (IAM), encryption, network policies, and firewalls.
- Recommended: Multicloud Management with Red Hat Advanced Cluster Management for Kubernetes (DO432), or equivalent experience with RHACM.

COURSE OBJECTIVES

By the end of this course, participants will be able to:

- **Impact on the Organization:** This course, DO505: Building a Sovereign Cloud with Red Hat OpenShift, is vital for organizations that must meet digital sovereignty requirements, such as the EU Cloud Sovereignty Framework, and operate multitenant cloud platforms. By providing deep expertise in key areas such as hosted control plane isolation, jurisdiction-aware identity and access controls, external key management, and cryptographic data protection across all three states, the course enables the organization to design and operate sovereign cloud platforms that satisfy regulatory mandates for data residency, personnel sovereignty, and cryptographic control. This expertise directly reduces the risk of regulatory noncompliance and ensures that the organization can offer sovereign clusters-as-a-service to tenants with verifiable jurisdictional guarantees.
- **Impact on the Individual:** For individuals, this course closes critical skill gaps by offering a deep, hands-on dive into building and operating sovereign cloud infrastructure on Red Hat OpenShift. Learners gain practical proficiency in deploying multitenant hosted control planes, enforcing zero-trust workload identity with SPIFFE and SPIRE, integrating external key management for cryptographic sovereignty, implementing network-bound disk encryption, and configuring jurisdiction-aware access controls. This mastery empowers the individual — whether an enterprise architect, IT security practitioner, or operations engineer — to confidently design and operate cloud platforms that meet stringent digital sovereignty requirements.

COURSE OUTLINE

Module 1: Introduction to Sovereign Cloud Operations

- Describe the four pillars of sovereignty, the European Union Sovereignty Objectives (SOV), and the Red Hat Advanced Cluster Management (RHACM) hub-and-spoke architecture within the context of sovereign cloud providers.

Module 2: Architecting the Sovereign Boundary

- Onboard and manage new sovereign cluster-as-a-service tenant clusters by using RHACM, and enforce zero-trust isolation, operational sovereignty, and jurisdictional access controls.

Module 3: Securing Sovereign Data

- Implement advanced cryptographic controls for tenant clusters and provider workloads to ensure data confidentiality at rest, in use, and during recovery.