

Building a Sovereign Cloud with Red Hat OpenShift (DO505)

ID DO505 Price 1,870.— €(excl. VAT) Duration 3 days

Who should attend

- 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

- Take our free assessment to gauge whether this offering is the best fit for your skills.
- [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

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

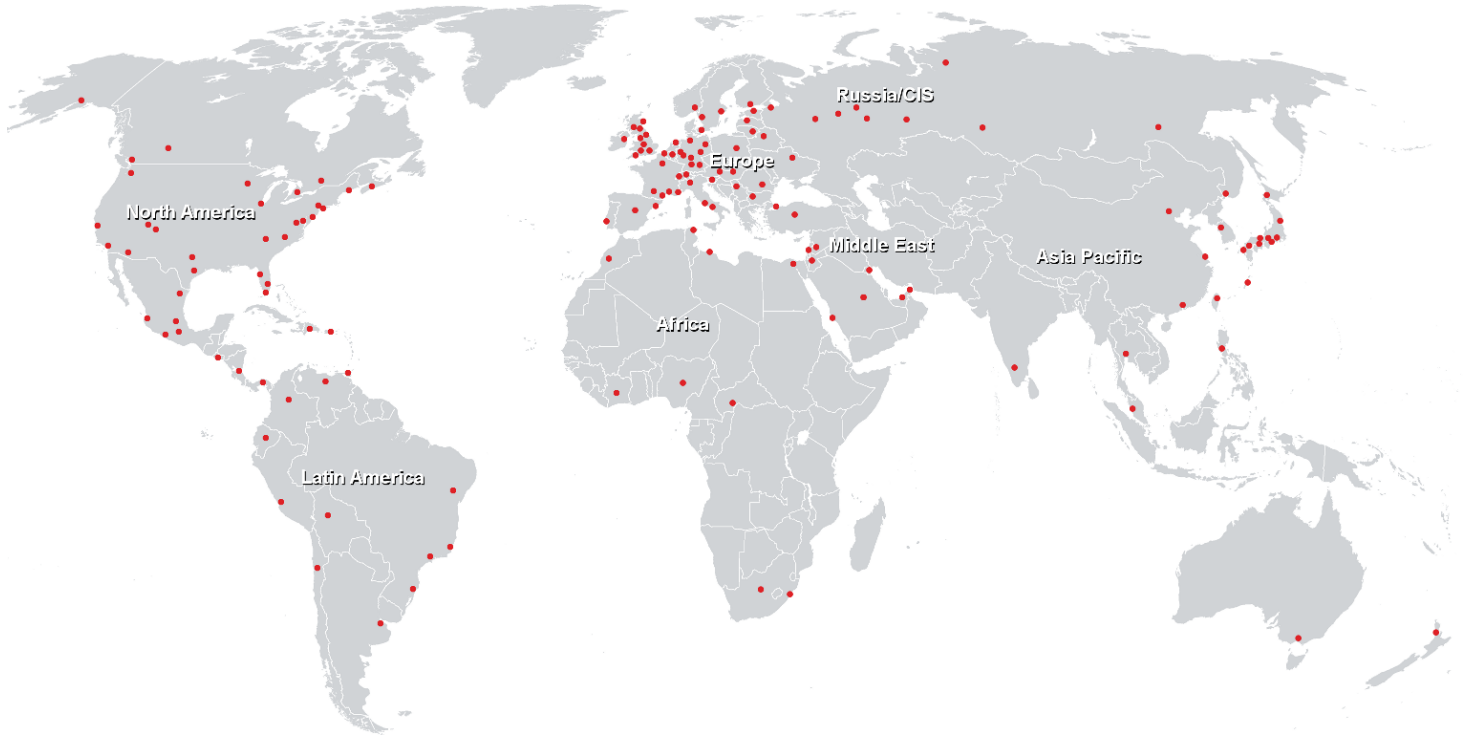
For individuals, this course closes critical skill gaps by offering a deep, hands-on dive into building and operating sovereign cloud infrastructure on Red Hat OpenShift. Learners gain practical proficiency in deploying multitenant hosted control planes, enforcing zero-trust workload identity with SPIFFE 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 Content

- Defining the pillars of digital sovereignty and mapping sovereignty objectives to a multicloud 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.

Building a Sovereign Cloud with Red Hat OpenShift (DO505)

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>