

Building a Sovereign Cloud with Red Hat OpenShift

Course code: D0505

As of January 2026, only in-person Red Hat training is available for purchase under the original terms. Virtual training (VT) courses are offered exclusively as part of the annual RHLS Course subscription can be found here. How to schedule a virtual course in the Red Hat Learning Subscription can be found here. 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.

Affiliate	Duration	Course price	ITB
Praha	3	1 905 €	0
Brno	3	1 905 €	0
Bratislava	3	1 905 €	0

The prices are without VAT.

Course terms

Date	Duration	Course price	Type	Course language	Location
------	----------	--------------	------	-----------------	----------

The prices are without VAT.

Who is the course for

- 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.

What we teach you

- 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.

Required skills

- 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 | D0280
- or equivalent experience with managing and troubleshooting a self-managed OpenShift cluster.

GOPAS Praha
Na Strži 2097/63
140 00 Praha 4 - Krč
Tel.: +420 226 201 390
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 530 513 590
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 902 903 132
info@gopas.sk



Copyright © 2026 GOPAS, a.s.,
All rights reserved

Building a Sovereign Cloud with Red Hat OpenShift

- 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 | D0432
- or equivalent experience with RHACM.

Course outline

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.

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.

Securing Sovereign Data

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

GOPAS Praha
Na Strži 2097/63
140 00 Praha 4 - Krč
Tel.: +420 226 201 390
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 530 513 590
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 902 903 132
info@gopas.sk



Copyright © 2026 GOPAS, a.s.,
All rights reserved