



Red Hat Security: Securing Containers and OpenShift

Code:	DO425
Length:	4 days
URL:	View Online

Red Hat Security: Securing Containers and OpenShift (DO425) is designed to help infrastructure administrators and security professionals learn to identify and mitigate threats to OpenShift container-based infrastructure. The curriculum also covers how to implement and manage secure architecture, policies, and procedures for modern containerized applications and software-defined networking. This course is based on Red Hat® Enterprise Linux® 7.5, Red Hat® OpenShift® Container Platform 3.11, and Red Hat® Identity Manager 7.5.

Skills Gained

As a result of attending this course, you should be able to use security technologies included in Red Hat OpenShift Container Platform and Red Hat Enterprise Linux to manage security risk and help meet compliance requirements. You should be able to demonstrate these skills:

- Use recommend practices to ensure that images for container deployment come from trusted sources, including the use of secure registries, signed images, secure access protocols, and authorized access controls.
- Explain and implement advanced SELinux techniques to restrict access by users, processes, and virtual machines.
- Configure security context constraints to control the actions that pods can perform and to declare what a pod has the ability to access.
- Implement the Linux computer security (seccomp) and Linux capabilities features to control the vulnerability footprint of a containerized application.
- Implement and configure single sign-on for web applications, including the use of JWT for token sharing.
- Explain and implement network isolation and encryption techniques to segregate application traffic to allow only authorized access.
- Implement and explain storage management techniques to segregate volume storage I/O to allow only authorized access.
- Observe and explain how the build process can be extended to include automated security testing and vulnerability scanning to ensure that no exploits are introduced into the final container images to be deployed.
- Manage container deployment policies and configuration to control application placement, resource capacity, container affinity, and application demand scaling.
- Manage OpenShift project access and quotas to ensure private and authorized self-service access, as well as to limit exposure to rogue tokens and denial-of-service attempts.

Who Can Benefit

This course is designed for professionals responsible for designing, implementing, maintaining, and managing the security of containerized applications on Red Hat Enterprise Linux systems and in Red Hat OpenShift Container Platform installations, including these roles:

- System administrators
- IT security administrators
- IT security engineers
- DevOps engineers
- Cloud developers
- Cloud architects

Prerequisites

- Become a Red Hat Certified Engineer (RHCE®), or demonstrate equivalent Red Hat Enterprise Linux knowledge and experience
- Become a Red Hat Certified Specialist in OpenShift Administration, or demonstrate equivalent Red Hat OpenShift Container Platform knowledge and experience

Course Details

Course Outline

Describe host security technologies Understand the core technologies that make Red Hat Enterprise Linux a robust and trusted container host. Establish trusted container images Describe the registries, services, and methods that comprise the Red Hat image ecosystem. Implement security in the build process Learn automated methods for integrating security checks into build and deployment pipelines. Manage user access control Apply methods for integrating and managing user authentication for operators and for web applications. Control the deployment environment Determine how a container platform secures the deployment process through policies and automation. Manage secure platform orchestration Study how a container platform secures the orchestration process through policies and infrastructure. Provide secure network I/O Discover the technologies and control features that enable multitenancy and project isolation. Deliver secure storage I/O Enable authorized, multitenant storage access through a firm understanding of related technologies and control features.

Download Whitepaper: Accelerate Your Modernization Efforts with a Cloud-Native Strategy

Get Your Free Copy Now