AMBIENT-IT

+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated on 19/12/2023

Sign up

OpenShift Advanced Training: Kubernetes Security

3 days (21 hours)

Presentation

Kubernetes open source software (commonly known as "K8s") is now the standard for container orchestration. This tool will enable you to enter the "Cloud Native" era and expose your applications on a large scale in a secure, reproducible and flexible way.

You'll also learn how to upgrade your applications to the micro-service, modular and scalable standard. Acclaimed by Silicon Valley giants, K8s is governed by the Cloud Native Computing Foundation (part of the Linux Foundation).

Kubernetes provides a "platform for automating the deployment, scaling and production release of application containers on server clusters". It supports multiple container execution engines, including Docker, Rocket and Singularity.

This training course covers advanced aspects of security in the Kubernetes ecosystem, focusing on the concrete example of OpenShift, one of the flagship Kubernetes distributions developed by RedHat. It covers security strategies, best practices and provides OpenShift-specific case studies for an in-depth understanding of securing Kubernetes clusters.

This course will introduce you to the latest version of Kubernetes (at the time of writing: Kubernetes 1.29).

Objectives

- End-to-end security: Understand best practices for securing each component of the lifecycle, from code development to end-user.

- Identification of Strategic Points: Analyze the crucial points to secure within a Kubernetes cluster, focusing on strategic areas that may be potential points of attack.
- Understanding Internal Functioning: Acquire an in-depth understanding of the internal workings of Kubernetes, including its inherent security mechanisms
- Vulnerability Detection: Learn to identify potential vulnerabilities within a Kubernetes cluster, with a focus on proactive detection techniques.
- Relevant Solutions: Acquire the skills needed to apply solutions from in response to identified vulnerabilities
- Securing Data and Application Load: Implement advanced strategies to secure sensitive data and ensure application load protection in a Kubernetes environment.
- OpenShift case studies: Apply the concepts learned to case studies specific to OpenShift. OpenShift, understanding how to adapt security measures to the particular characteristics of this platform

Target audience

- Developers
- CISO
- **Safety experts**
- System administrators
- DevOps
- Architects

Prerequisites

Good knowledge of a Unix system, the standard Kubernetes API and Linux containers.

Our OpenShift Advanced training program

Administration of Kubernetes in Production

- The inner workings of the Kubernetes/OpenShift Control-Plane
- Advanced Kubernetes/OpenShift configuration for production, with a focus on pod security.
- Semi-automated configuration of an On-Premise Kubernetes cluster
- High availability and Control-Plane Rolling Upgrade
- The OpenShift Machine API operator and the ClusterAutoscaler

Kubernetes architecture

- Control plane components and work nodes
- How the reconciliation loop and Kubernetes Controller work
- Operating etcd in high-availability mode

- Internal operation of the API server: authentication, authorization and Admission Control
- Admission controllers (MutatingWebhook and ValidatingWebhook)
- Description of the Kubernetes Scheduler algorithm, predicates and priorities
- Declarative configuration
- Kinematics of Pod creation from Deployment
- Kube-proxy: advanced operation of the Services virtual network
- Service discovery with CoreDNS
- Description of the internal structure of a Pod and the infrastructure container

Securing the API server

- Authentication: ServiceAccount, certificates, tokens, and Dex
- Setting up the Kubeconfig file with Configuration Contexts
- Securing the Kubernetes API: authentication, authorization and Admission Control. Putting the OpenShift configuration into perspective
- API access rights with RBAC: Role And ClusterRole, RoleBinding And ClusterRoleBinding
- Case studies

System security

- Secure execution of Unix processes in Pods (SecurityContex)
- Industrialization of Pod security withPodSecurity and/or OPA GateKeeper.
- Default security levels: Kubernetes vs OpenShift (SecurityContextConstraints)
- Distroless and rootless containers

Network security

- Choosing a secure, efficient CNI network plug-in
- Industrialization of network security (L4) with NetworkPolicies (ingress and egress) and TLS

Network quality

- Optimum use of material resources with Requests and Limits, ResourceQuota and LimitRanges
- QoS classes: Guaranteed, Burstable and BestEffort
- Configuring the Kubernetes scheduler with Taints and Affinities

Case studies

- Kubernetes pentesting case study.
- Secure application management, with GitOps-oriented CI/CD
- Secure storage management (PersistentVolume, PersistentVolumesClaim, StorageClass), and dynamic volume provisioning.
- Presentation of advanced features in Sysdig and/or Calico (optional)

Monitoring

- Monitoring and logging objectives
- Automate monitoring with Prometheus operator
- Obtain and aggregate metrics for your cluster and applications
- AlertManager: alert management and routing
- Visualize and interact with your data with Grafana

Complementary module (+1 day)

Companies concerned

This training course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced computer technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the training to come, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical course: 60% Practical, 40% Theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples, with brainstorming sessions and group work.

Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

Sanction

A certificate will be issued to each trainee who completes the course.