Kubernetes Security and CI/CD

Duration: 10 days (8hrs/day)

Prerequisites:

- Basic knowledge of Linux Server Administration.
- Basic knowledge of Containers

Course Objective: This comprehensive DevOps Tools course, covering implementation of container orchestration and managing containerized application with CI/CD pipeline and security best practices, is designed to equip learners with the skills needed to successfully to implement DevOps practices securely.

Kubernetes and DevOps Tools Version: Latest

Lab Requirement: Koenig-DC and AWS EKS

Module 1 – Kubernetes Recap [16 - hours]

Overview of Container Orchestration

Introduction to Kubernetes

Understanding Kubernetes Architecture

Lab: Installation of Kubernetes 1-Master and 2-Nodes Cluster

Lab: Choose a Network Solution and Configure

Lab: Verify Installation with Kubectl command

Understanding Pods, Labels & Selectors

Lab: Deploying Applications as a Pod

Lab: Managing Labels & Selector

Understanding Replica Set

Lab: Deploying Replica Set

Understanding Services – ClusterIP, NodePort & LoadBalancer

Lab: Creating & Managing Service

Understanding Daemon Sets

Lab: Deploying Applications as Daemon Sets

Overview of Deployment

Deployment Strategies – Blue/Green & Canary

Lab: Deploying Applications as Deployment

Lab: Implementing Deployment Strategies on Deployments

Understanding Volume Management in K8s

Types of Volumes Provisioning

Persistent Volumes

Persistent Volume Claim

Lab: Using PV & PVC to attach Persistent Volume to a Pod as HostPath

Understanding Kubernetes Authentication

Lab: Creating Service Accounts

Understanding Role, ClusterRole, RoleBinding& ClusterRoleBinding

Lab: Managing Roles and Role Binding

Lab: Managing Cluster Role and Cluster Role Binding

Understand Basics of Kubernetes Networking

Understand CNI overview

Understand Pod Networking Concepts

Understanding DNS of K8s

Understanding Ingress

Lab: Configure and Manage Ingress Rule

Understanding Namespace & Use-Cases

Lab: Creating Namespace & Deploying K8s resources in Different Namespaces

Metal Load Balancer

Lab: Deploying Metal Load Balancer

Module 2 – Kubernetes Extras [12 - hours]

Introduction to StatefulSet

Use cases of StatefulSet

Manage StatefulSet

Storage in StatefulSet

Lab: Deploying and Managing Stateful Sets

Lab: Creating Persistent Storage in Stateful Sets

Headless Service

Lab: Headless Service

Introduction to Readiness and Liveness Probe

Implement Readiness and Liveness in Pod

Lab: Creating Liveness and Readiness Probe for Pod

Kubernetes Autoscaling using VPA, HPA, CA and Karpenter

Lab: Implementing VPA in EKS cluster

Lab: Implementing HPA in EKS cluster

Lab: Implementing cluster node autoscaling

Lab: Implementing cluster node autoscaling using Karpenter

Understanding Kubernetes package manager – Helm

Lab: Deploying application using Helm

Module 3 - Cluster Hardening [10 - hours]

Use CIS Benchmark to Review the Security Configuration of Kubernetes Components

Lab: Perform Security Benchmark checks using CIS-CAT Lite and Kube-Bench Tool

Pod to Pod Communica1on

Public Key Infrastructure (PKI) – Certificate Authority (CA)

Lab: Find Certificates

Lab: Implementing Network Policies on Pods

Lab: Create User and assign RBAC (Role Based Access Control)

Lab: Disable Automount Service Account Token and Anonymous Access

Lab: Node Restriction Admission Controller

Module 4 - Minimize Microservice Vulnerabilities [10 - hours]

Managing Secrets

Lab: Managing Secrets

Lab: Encrypt Secrets in ETCD

Setup Appropriate OS Level Security Domains using PSP, OPA, Security Contexts

Lab: Implementing Security Context in Pods and Containers

Lab: Creating privileged containers using security context

Lab: Disable Privilege Escalation

Pod Security Policy

Container Runtime Sandboxes

Open Container Initiative

Kata Containers - Sandbox

Lab: Contact the Linux Kernel of worker node From Inside a Container

Lab: Implemen1ng Gvisor on pods

Lab: Custom Security Policies using OPA Gatekeeper

Module 5 - Supply Chain Security [10 - hours]

Container Image creation using Dockerfile

Lab: Creating container image using Dockerfile

Minimize Base Image Footprint Use Static Analysis of User Workloads (e.g. Kubernetes Resources and Docker Files)

Lab: Static Analysis with Kubesec

Lab: Static Analysis with OPA Conftest

Lab: Checking Image Vulnerabilities with Trivy

Secure Supply Chain

Lab: Whitelist Some Registries Using OPA

ImagePolicyWebhook

Lab: ImagePolicyWebhook

Module 6 – CI/CD with Jenkins, GitLab and ArgoCD [10 - hours]

What is CI/CD

Introduction to Jenkins

Lab: Jenkins Installation

Jenkins Management

Lab: Run Jobs on Remote Machines

Introduction to Jenkins Pipeline

Lab: Building Jenkins Pipeline

Introduction to Gitlab

Gitlab Architecture and Runner

Lab: Installing and Configuring Gitlab Runner

Lab: Building a CI-CD Pipeline Using Gitlab

Introduction JFrog Artifactory

Lab: Deploying artifacts with JFrog

What and why of ArgoCD

ArgoCD Architecture

Lab: Installing and configuring ArgoCD

Lab: Deploying Java application on Kubernetes using ArgoCD

Module 7 – Service mesh tool – Istio [06 - hours]

What and why of service mesh

Service mesh architecture

Admission controller

Sidecar containers

Lab: Istio installation and configuration

Lab: Configure traffic management, virtual services, mutual TLS [mTLS] and Observability

Service mesh vs Ingress

Module 8 – Logging and Monitoring [04 - hours]

Understand how to Monitor Application and Cluster Components

Lab: Understand how to Read Application & Cluster Component Logs

Lab: Deploying Prometheus & Grafana to Monitor K8s Cluster

Lab: Monitoring k8s with Zabbix

Module 9 – Managing multi Kubernetes cluster with Rancher [02 - hours]

Rancher overview

Lab: Importing Kubernetes cluster to Rancher

Exploring available external authentication to Rancher