Koenig Crafted – Kubernetes Administration and Security (CKA + CKS)

Duration: 8 Days

Hands-On Format: This hands-on class is approximately 80/20 lab to lecture ratio, combining engaging lecture, demos, group activities and discussions with comprehensive machine-based practical programming labs and project work.

Module 1 – Core Concepts

Overview of Container Orchestration
Introduction to Kubernetes
Kubernetes Architecture

Module 2 – Installation, Configuration & Validation

Design a Kubernetes Cluster
Installation of Kubernetes Master and Nodes
Choose a Network Solution
Verify Installation

Module 3 – Managing Resources

Managing Pods
Managing Labels & Selector
Managing Replication Controller & Replica Set
Managing Service – ClusterIP, NodePort, LoadBalancer

Module 4 – Application Lifecycle Management

Overview of Deployment
Deployment Strategies
Managing Deployment
Canary Deployment
Blue-Green Deployment

Module 5 – Environment Variable

Plain Key
Config Map
Secret

Module 6 – Storage

Volumes
Persistent Volumes
Persistent Volume Claim

Module 7 – Security

Kubernetes Authentication
Managing Users in Kubernetes
Service Account
Managing Roles and Role Binding

Managing Cluster Role and Cluster Role Binding
Security Context
Network Policies

Module 8 – Cluster Maintenance

OS Upgrade
Upgrade Cluster Version
Static Pod
ETCD Backup
Jobs and Cron Job

Module 9 – Logging and Monitoring

Understand how to Monitor all Cluster Components
Understand how to Monitor Applications
Manage Cluster Components Logs
Manage Application Logs
Logging with Elasticsearch
Monitoring with Prometheus and Grafana

Module 10 – Networking in Kubernetes

Kubernetes Networking
Understand CNI
Understand Pod Networking Concepts
Configure and Manage Ingress Rule
Configure Ingress with TLS
Namespace
Metal Load Balancer

Module 11 – Troubleshooting

Troubleshoot ETCD Failure
Troubleshoot Kubelet Failure
Troubleshoot Container Runtime Failure
Troubleshoot Scheduler Failure

Module 12 – Cluster Hardening

Use CIS Benchmark to Review the Security Configuration of Kubernetes Components
Minimize Use of, and Access to, GUI Elements
Exercise Caution in Using Service Accounts e.g., Disable Defaults, Minimize Permissions on Newly Created Ones

Module 13 – System Hardening

Minimize Host OS Footprint (Reduce Attach Surface)
Minimize IAM Roles
Minimize External Access to the Network
Appropriately Use Kernel Hardening Tools Such as App Armor, Seccomp

Module 14 – Minimize Microservice Vulnerabilities and Supply Chain Security

Setup Appropriate OS Level Security Domains e.g. Using PSP, OPA, Security Contexts
Use GVisor
Minimize Base Image Footprint
Use Static Analysis of User Workloads (e.g. Kubernetes Resources, Docker Files) Scan Images for Known Vulnerabilities

Module 15 – Monitoring, Logging and Runtime Security

Perform Behavioral Analytics of Syscall Process and File Activities at the Host and Container Level to Detect Malicious Activities
Detect Threats within Physical Infrastructure, Apps, Networks, Data, Users and Workloads
Detect All Phases of Attack Regardless Where It Occurs and How It Works
Perform Deep Analytical Investigation and Identification of Bad Actors within Environment Ensure Immutability of Containers at Runtime
Use Audit Logs to Monitor Access