**Training Schedule – Advance Level Kubernetes – On AWS EKS**

**Prerequisites:**

* Linux/Unix Systems Fundaments
* Familiarity with Command Line Interface (CLI)
* Fundamental knowledge of editors on Linux (any one of vi/nano/emacs)
* Familiarity with at least one scripting/programming language

**Out Come:**

After attending this training, the trainees will be gaining the below skills on Docker and Kubernetes,

* Docker Architecture and Understanding
* Install and Configure Docker
* Build Custom Images
* Manage Container Lifecycle
* Kubernetes Container Orchestration fundamentals
* Installing and Configuring Kubernetes cluster
* Deploying and Scaling Cluster apps
* Understand the Pods, Volumes and Services in Kubernetes
* Secrets and ConfigMaps using Kubernetes
* Scheduling Container Applications
* Auditing and Troubleshooting Kubernetes Cluster
* Kubernetes best Security Practices
* Creating YAML Files for the Kubernetes Deployments , Services.

|  |  |
| --- | --- |
| **Local setup for Remote Connect** | **Remote Lab Setup** |
| Laptop/Desktop with high-speed internet  connection | OS: CentOS8 |
| Memory: 4 GB RAM | Memory: 32 GB RAM |
| CPU: 1 CPU Cores | CPU: 8 CPU Cores |
| Storage: 20 GB | Storage: 500 GB SSD |

**Day 1:**

1. **Kubernetes Platform**

* Comparison with Docker Swarm
* Orchestration and Various Tools
* History of Kubernetes
* Features of Kubernetes
* What Kubernetes is not!
* Kubernetes Versions

1. **Kubernetes Architecture**

* Kubernetes Terminology
* Kubernetes Components
* Kubernetes Cluster Architecture
* Understanding Kubernetes Master Components
* Kube-apiserver
* ETCD
* Kube-scheduler
* Kube-controller
* Kube-DNS
* Understanding Kubernetes Node Components
* Kube-proxy
* Kubelet
* Container Runtime
* Kubernetes Secure Architecture
  + Intro
  + Practice - Find various K8s certificates

**3. Create your k8s cluster**

* Practice - Create AWS Account
* Practice - Configure " aws ecs create-cluster --cluster-name MyCluster" command
* Practice - Create Kubeadm Cluster
* Practice - Firewall rules for NodePorts
* Notice: Always stop your instances
* Containerd Course Upgrade

**4. Foundation Container in the hood**

* Container Tools Introduction
* Practice - The PID Namespace
* TEST - Docker Container Namespaces
* TEST - Podman Container Namespaces

**5. Cluster Setup Network Policy**

* Cluster Reset
* Practice - Backend to Database traffic
* TEST - Default-Deny Network Policy
* TEST - NetworkPolicy Namespace Communication

**6. Cluster Setup Gui Element**

* Introduction
* Practice - Install Dashboard
* Practice - Outside Insecure Access
* Practice - RBAC for the Dashboard

**7. Kubernetes Setup and Validation**

* Understanding different tools for deploying Kubernetes Cluster
* Release Binaries, Provisioning and Types of Clusters
* Building the Kubernetes Cluster using kubeadm
* Installing Kubernetes Master and Nodes
* Configuring Secure Cluster Communications
* Testing the Cluster

**Lab:** Deploying Kubernetes Cluster using EKS

**Lab:** Adding Nodes to Kubernetes Cluster

**Lab:** Deploying and Accessing Kubernetes Dashboard Service

**8. Working with Pod**

* Pod Overview
* Understanding Pod Lifecycle
* Multi-container Pod
* Static Pod
* Init Containers
* Labels, Selectors & Annotations

**Lab:** Imperative Commands and Formatting Output with kubectl

**Lab:** Working with Single Container Pods

**Lab:** Creating multi container Pod

**Lab:** Creating init container Pod

**Lab:** Working with Static Pod

**Day 2:**

**1. Kubernetes Networking and Service**

* Cluster Communications
* Pod and Node Networking
* Container Network Interface (CNI)
* Service Networking: ClusterIP, NodePort & Load Balancer
* Ingress Rules
* Cluster DNS
* Network Policies

**Lab:** Exposing Applications using various types of Services

**Lab:** Install and Configure Ingress Controller

**Lab:** Create Network Policies to control traffic flow

**2. Application Lifecycle Management**

* Pods: Single Container, Multi Container, Static, Init
* Deploying Applications in the Kubernetes Cluster
* Controllers: RS and Deployment
* Deploying an Application, Rolling Updates, and Rollbacks
* Configuring an Application for High Availability and Scale
* Imperative Commands & Manifests (YML Intro)

**Lab:** Deploying Application using Replication Controller

**Lab:** Deploying Application using Replica Set

**Lab:** Rolling Updates and Rollbacks using Deployment

**Lab:** Deploying Application using Daemon Set

**Lab:** Deploying StatefulSet Application

**Lab:** Deploying Multi-Tier Application

**3. Working with Kubernetes Scheduler**

* Pod Scheduling within the Kubernetes Cluster
* Configuring the Kubernetes Scheduler
* Running Multiple Schedulers for Multiple Pods
* Taints, Tolerances, Node Selector, labels & Selectors
* Scheduling Pods with Resource Limits and Label Selectors
* Displaying Scheduler Events

**Lab:** Manually scheduling Pod

**Lab:** Scheduling Pod based on Node Selector and Labels

**Lab:** Taints and Tolerations

**Lab:** Working with Affinity and Anti-Affinity

**4. Storage**

* Managing Data in the Kubernetes Cluster
* EmptyDir, hostPath, PV, PVC
* Volume Access Modes
* Applications with Persistent Storage
* ConfigMaps, Secrets

**Lab:** Working with Kubernetes Volume Service

**Lab:** Working with ConfigMaps and Secrets

**Day 3:**

**1. Logging and Monitoring**

* Describe Resources
* Pod/container logs
* Metric Server & top command
* Events

**Lab**: Working on Logs and Events

**Lab**: Working with Metric Server

**Lab**: Working with HPA

**2. Managing Cluster**

* Managing the Kubernetes Cluster
* Upgrading the Kubernetes Cluster
* Backing Up and Restoring a Kubernetes Cluster

**Lab:** Upgrading Kubernetes Cluster

**3. Troubleshooting**

* Control Plane Failures
* Node Failure
* Application Failure
* Components manifests and errors
* Scenarios and Solutions

**Lab:** Troubleshooting in Kubernetes

**4. Cluster Setup Secure Ingress**  :

* K8s Docs in correct Version
* Introduction
* Practice - Create an Ingress
* Practice - Secure an Ingress
* TEST - Create an Ingress
* TEST - Secure an Ingress

**Day 4:**

**1. Cluster Setup Node Metadata Protection**

Introduction

Practice: Access Node Metadata

Practice: Protect Node Metadata via NetworkPolicy

TEST - NetworkPolicy Metadata Protection

**2. Cluster Setup CIS BenchMark**

introduction

Practice - CIS in Action

Practice - kube-bench

Recap

TEST - Apply CIS rules for Controlplane

**3. Cluster Setup Verify Platform Binary**

Introduction

Practice - Download and verify K8s release

Practice - Verify apiserver binary running in our cluster

TEST - Verify Kubelet Binary

**4. Cluster Hardening RBAC**

Intro

Practice - Role and Rolebinding

Practice - ClusterRole and ClusterRoleBinding

Accounts and Users

Practice - CertificateSigningRequests

Recap

TEST - RBAC ServiceAccount Permissions

TEST - RBAC User Permissions

TEST - CertificateSigningRequests Sign Manually

TEST - CertificateSigningRequests Sign via API

**5. Cluster Hasrdening Exercise caution in using Service Account**

Introduction

Practice - Pod uses custom ServiceAccount

Practice - Disable ServiceAccount mounting

Practice - Limit ServiceAccounts using RBAC

Recap

TEST - ServiceAccount Token Mounting

**Day 5:**

**1. Cluster hardening: Restrict APi Access**

Introduction

Practice - Anonymous Access

Practice - Insecure Access

Practice - Manual API Request

Practice - External Apiserver Access

NodeRestriction AdmissionController

Practice - Verify NodeRestriction

Recap

TEST - Crash that Apiserver

TEST - Apiserver Manifest Misconfigured

TEST - NodeRestriction

**2. Cluster Hardening Upgrade K8s**

Introduction

Ubuntu 20.04 Update

Practice - Create outdated cluster

Practice - Upgrade controlplane node

Practice - Upgrade node

**3. Micro service vulnerability Manager Secret**

Introduction

Practice - Create Simple Secret Scenario

Practice - Hack Secrets in Container Runtime

Practice - Hack Secrets in ETCD

ETCD Encryption

Practice - Encrypt ETCD

Recap

TEST - Access Secrets in Pods

TEST - Read Secret Values

TEST - Secrets Pods and ServiceAccount

TEST - ETCD Encryption

**4. Micro service vulnerability -container runtime sandbox**

practice - Container calls Linux Kernel

Open Container Initiative OCI

Sandbox Runtime Katacontainers

Sandbox Runtime gVisor

Practice - Create and use RuntimeClasses

Practice - Install and use gVisor

Recap

TEST - gVisor and RuntimeClass

**5. Micro service vulnerability** -OS level

intro and Security Contexts

Practice - Set Container User and Group

Practice - Force Container Non-Root

Privileged Containers

Practice - Create Privileged Containers

PrivilegeEscalation

Practice - Disable PrivilegeEscalation

TEST - Privileged Containers

TEST - Privilege Escalation Containers

**6. Microservice vulnerability-Mtls**

Intro

Practice - Create sidecar proxy

**7. Open Policy Agent**

Cluster Reset

Introduction

Practice - Install OPA

Practice - Deny All Policy

Practice - Enforce Namespace Labels

Practice - Enforce Deployment replica count

Practice - The Rego Playground and more examples

**8. Supply Chain Security Image Footprint**

introduction

Practice - Reduce Image Footprint with Multi-Stage

Practice - Secure and harden Images

TEST - Image Footprint User

TEST - Image Container Hardening

Supply chain Security Static Analysis

introduction

Kubesec

Practice - Kubesec

OPA Conftest

Practice - OPA Conftest for K8s YAML

Practice - OPA Conftest for Dockerfile

TEST - Manual Static Analysis K8s

TEST - Manual Static Analysis Docker

**9. Supply Chain Security Image Vulnerability**

Introduction

Clair and Trivy

Practice - Use Trivy to scan images

Recap

TEST - Scan images using Trivy

**10. Supply chain security secure supply chain**

Introduction

Practice - Image Digest

Practice - Whitelist Registries with OPA

ImagePolicyWebhook

Practice - ImagePolicyWebhook

TEST - Complete ImagePolicyWebhook Setup

TEST - Use Image Digest

**11. Runtime Security behavior analysis at host and container**

introduction

Practice - Strace

Practice - Strace and /proc on ETCD

Practice - /proc and env variables

Practice - Falco and Installation

Practice - Use Falco to find malicious processes

Practice - Investigate Falco rules

Practice - Change Falco Rule

**12**. **Runtime Security-immutable container**

Introduction

Ways to enforce immutability

Practice - StartupProbe changes container

Practice - SecurityContext renders container immutable

TEST - Immutability Readonly Filesystem

**13. Runtime security auditing**

Introduction

Practice - Enable Audit Logging in Apiserver

Practice - Create Secret and check Audit Logs

Practice - Create advanced Audit Policy

**14. CI/CD Pipeline Setup With Jenkins , Docker, Kubernetes**

**15. Creating a EKS Cluster with Terraform.**

**16. Servicemesh**