Kafka Security

Prerequisites: Basic knowledge of Kafka

Duration: 1 Day (8 Hrs./Day)

Course Objective: This course aims to provide a comprehensive understanding of securing Apache Kafka deployments. Participants will learn about Kafka's authentication, authorization, and encryption mechanisms, including SSL, SASL_SSL, and Kerberos. The course will cover best practices for securing Kafka, including Kraft and audit logs. Hands-on labs will guide participants through practical setups of SSL and Kerberos security, creating certificate authorities, configuring clients, and managing access control lists (ACLs).

Apache Kafka version: Latest.

Lab Requirement: Koenig DC/Linux (CentOS 9) (customizable).

Module 1 - Introduction to Kafka Security

Kafka Authentication Basics

Kafka Authentication with SSL and SASL_SSL

Authorization

Encryption

Securing Kraft

Audit Logs

Security Recommendations

Lab: Kafka cluster setup

Module 2 – Kafka security hands on

Lab: Creating a Certificate Authority (CA)

Lab: SSL Setup in Kafka

Lab: SSL Setup for Clients

Lab: SSL Authentication

Lab: Hands-On Kerberos - Part 1: Setup Azure Virtual Machines

Lab: Hands-On Kerberos - Part 2: Principals & Keytabs

Lab: Hands-On Kerberos - Part 3: Kafka Configuration

Lab: Hands-On Kerberos - Part 4: Client Configuration

Lab: JAAS file / config

Lab: Hands-On ACL demo