

Kafka Security with Kerberos

TLS, SASL/GSSAPI and access-control labs

FA-0738 · 3 days

Cybersecurity · DevOps, Cloud & Infrastructure

Introduction

Learn to configure and test Kafka encryption, authentication and access controls in a guided lab. The course combines TLS certificates, Kerberos principals and keytabs, broker/client configuration and ACL demonstrations.

Current Kafka exercises use a compatible KRaft-based environment. ZooKeeper security is covered separately for understanding legacy Kafka deployments.

Learning outcomes

- Distinguish transport encryption, authentication and authorisation in Kafka.
- Configure and test TLS for brokers and clients, including certificate trust and client authentication.
- Use Kerberos/GSSAPI principals and keytabs with Kafka SASL configuration.
- Apply and test Kafka ACLs for selected client operations.
- Explain ZooKeeper security considerations for legacy deployments and identify cluster-security dependencies.

Prerequisites

- Basic Kafka producer/consumer and cluster knowledge.
- Linux command-line skills and familiarity with service configuration.
- Access to the designated Kafka and Kerberos lab environment.

Training outline

1. Day 1 — Kafka Setup and TLS

- Kafka security overview and lab structure.
- Set up a compatible Kafka environment and verify console producer/consumer operation.
- Contrast KRaft setup with the ZooKeeper-based legacy architecture.
- TLS encryption, certificate authorities, broker certificates and client trust.
- Create a lab CA and configure broker/client TLS; verify hostname and trust behaviour.
- Configure certificate-based client authentication and test connections.

2. Day 2 — Kerberos and SASL Authentication

- SASL mechanisms and the role of GSSAPI/Kerberos.
- Prepare the lab Kerberos service and relevant naming/configuration dependencies.
- Create broker and client principals and keytabs.
- Configure Kafka broker and client JAAS/SASL settings and test authenticated production/consumption.
- Distinguish SASL authentication from TLS transport encryption; use a compatible SASL_SSL configuration in the combined lab.

3. Day 3 — Authorisation and Cluster Security

- Kafka ACL resources, principals and operations.
- Configure the appropriate KRaft authorizer and demonstrate allowed and denied client operations.
- Legacy ZooKeeper security: principals, Kerberos configuration, znodes and ACLs.
- Discuss ZooKeeper privileged users and legacy security-migration tooling in version context.
- Cluster security review: client, inter-broker and controller communication, credential handling and configuration checks.
- Review practical results and troubleshoot selected authentication/authorisation failures.