Security Enablement

Engagement Objectives
The goal of this consulting engagement is for a Confluent Kafka expert to work alongside your technical teams to analyze your security requirements and discuss Kafka security concepts and to share best practices and known pitfalls. You’ll work through an architectural design, associated configurations and a deployment plan, evaluating and testing options on a test cluster to ensure you have everything required to deploy successfully.

By engaging with Confluent Professional Services, you leverage our expertise, knowledge and experience to ensure your security implementation is best tailored for your use cases, giving you confidence in the process.

Who Should Be Involved?
Engineers and operations staff responsible for Kafka security.

Prerequisites
» An existing deployment of Kafka version 0.9 or newer
» An understanding of your security requirements:
  • Do you need authentication, and if so, by SSL, SASL/Kerberos or SASL/Plain?
  • Do you need on-the-wire encryption? Between brokers? Between brokers and clients?
  • Do you need asymmetric encryption on brokers?
  • Do you need brokers to authenticate each other?
  • Do you need the client to authenticate the broker?
  • What security requirements do you have for other Confluent Platform components? Eg, Schema Registry, REST Proxy, ZooKeeper, Confluent Control Center
    • Who are the Kafka and Confluent Platform users? What privileges will they need?
  » For SASL Kerberos authentication you will need an existing Kerberos KDC or Active Directory server, and we will need to create principals and keytabs for brokers and clients.
  » For SSL/TLS, set up a trust store with either certificates or certificate authorities (CA).

Project Activities
» Preengagement survey and kickoff call
  • Align on engagement expectations and goals
  • Confirm logistics
» Discuss your existing Confluent Platform or Kafka architecture and use cases
» Discuss your security requirement goals encryption, authentication, and authorization
  • Testing
  • Secure a test Kafka cluster according to requirements
  • Secure other Confluent Platform components according to requirements
  • Define ACLs on Kafka topics according to requirements
  • Work with your engineers to implement security one producer and one consumer
  • Validate security on the test cluster
» Discuss implications of a rolling upgrade, if required
» Postengagement report delivery
  • Survey and follow-up call
Knowledge Transfer
At the end of the project, the Confluent engineer will provide a written summary of their recommendations, which may include:

1. An architectural design that implements your security requirements
2. Any configurations required to implement the architectural design
3. A deployment plan to guide you in implementing the design across your environments
4. Any additional recommendations that may be of use

Project Duration
One day of direct, continuous interaction between a Confluent engineer and the appropriate members of your technical team.

Project Location
Onsite at customer’s premises, a room with a whiteboard and a screen, or projector.

More Information
To discuss the Kafka Security Enablement Consulting service, or any of the other services and training courses offered by Confluent, please contact us at contact@confluent.io.