CONFLUENT PLATFORM

Enterprise-grade security

Confluent Platform completes Apache Kafka® with enterprise-grade security capabilities to ensure confidentiality of critical information, traceability of user actions and secure access to resources with scalability and standardization.

Ensure confidentiality and compliance

Enable granular access to critical resources

Simplify enterprise-scale operations

Standardize security across the platform

Why enterprise-grade security?

As companies from every size become digital, security hacks and data breaches have become a major concern and threat. Fragile systems can be exploited by malicious actors, impacted by poor quality controls, and taken down by both internal or external forces. This can halt operations, damage revenue streams, and tarnish an organization's reputation in front of customers and partners.

Modern companies embrace security and compliance as design principles. For organizations planning to use Kafka in production, this is no different. However, as an open source project, Kafka is not particularly well equipped to handle the requirements of an enterprise.

Confluent Platform offers a comprehensive set of security capabilities, so you can deploy Kafka confidently in production for mission-critical use cases.

Features

Secret Protection

Secret Protection safeguards all critically sensitive information (e.g passwords and tokens) within Kafka with at-rest encryption of configuration files. It encrypts not only Kafka files, but any config file published to Kafka.

Structured Audit Logs

Structured Audit Logs captures authorization logs in a set of dedicated Kafka topics, on a local or a remote cluster. Use Kafka native tools, such as ksqlDB, to process and analyze, or offload to external systems using Confluent connectors.

Role-Based Access Control

RBAC is a centralized implementation for secure access to Kafka resources with fine-tuned granularity and platform-wide standardization. Control permissions by users/groups to clusters, topics, consumers groups and even individual connectors.

BANK BRI

"With Confluent Platform and Kafka integrated into our stack, we're now able to detect and stop fraud in real time. We're the first bank in Indonesia with this capability, and it is already reducing fraud by blocking cards compromised by skimmers."

Kaspar Situmorang | Executive Vice President, Bank Rakyat Indonesia

Solution

Ensure confidentiality and compliance

Protect critically sensitive information

Avoid risk by ensuring that confidential information, such as user passwords, is only visible to authorized users. Secret Protection provides:

- At-rest encryption for any configuration file published to Kafka
- Support across all Confluent Platform components (Connect, ksqlDB, Schema Registry, REST Proxy and Control Center)

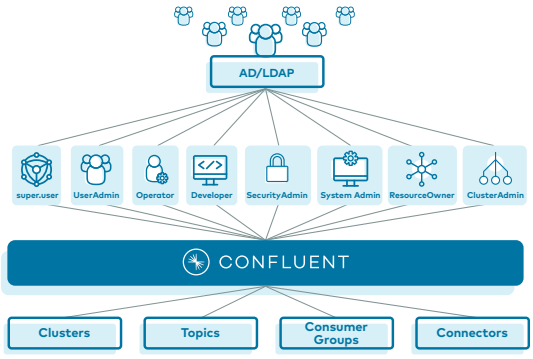
Trace user actions to conduct forensics

Capture the actions taken by users to detect abnormal behavior, identify potential security threats, and address compliance requirements related to information security. Structured Audit Logs allows you:

- Store authorization logs in dedicated Kafka topics
- Manage the type of logs that need to be traced
- Process and analyze using ksqlDB, or offload to external systems using Confluent sink connectors

To provide industry-backed standardization, Structured Audit Logs uses the CloudEvents specification to define the log syntax.

Role-Based Access Control provides platform-wide security with fine-tuned granularity.



Simplify enterprise-scale Kafka operations

Scale Kafka security management efficiently

Delegate the responsibility of managing access permissions to true resource owners, such as departments and business units. RBAC helps you scale Kafka more efficiently, because it spreads the operational load of managing authorization across a variety of users, which eliminates bottlenecks.

Manage Kafka centrally and visually

Simplifies security management across your organization by using Control Center to view your own permissions, as well as manage role bindings for your downstream stakeholders.

Enable granular access to critical resources

Build multi-tenant Kafka clusters

Control permissions by users and groups to shared platform resources, such as clusters, topics, and even individual connectors. RBAC allows you to run multi-tenant clusters, allowing for more scalable operations and more efficient use of resources.

Integrate with enterprise security systems

RBAC integrates with existing security authorization systems (AD/LDAP) to allow you to naturally handle permissions using a common user inventory across existing IT systems.

Standardize security across the platform

Leverage a single framework to centrally manage and enforce security authorization across the entire Confluent Platform to ensure security at scale. RBAC delivers comprehensive authorization enforced via:

- All user interfaces: GUI, CLI, and APIs
- All Confluent Platform components: Control Center, Kafka Connect, ksqlDB, Schema Registry, and REST Proxy

Confluent Platform. Enterprise event streaming platform built by the original creators of Apache Kafka. For more information, please visit **confluent.io**. To contact us, visit **confluent.io/contact**. For detailed product specifications, please refer to our **documentation**.