Dưới đây là giải thích chi tiết về từng dòng cấu hình bạn đã cung cấp trong file server.properties của Kafka:

**1. listeners=SASL\_PLAINTEXT://localhost:9092**

* **Ý nghĩa**: Định nghĩa các listener mà Kafka sẽ sử dụng để chấp nhận các kết nối từ client. Ở đây, listener được đặt tên là SASL\_PLAINTEXT, cho phép kết nối qua giao thức SASL mà không sử dụng mã hóa (PLAINTEXT). Kafka sẽ lắng nghe trên địa chỉ localhost với cổng 9092.

**2. advertised.listeners=SASL\_PLAINTEXT://localhost:9092**

* **Ý nghĩa**: Đây là danh sách các listener mà Kafka sẽ công bố đến các client. Thông tin này được sử dụng bởi các client để kết nối đến broker. Khi client yêu cầu thông tin broker, Kafka sẽ cung cấp địa chỉ này. Cũng như ở trên, listener này sử dụng SASL\_PLAINTEXT trên localhost:9092.

**3. inter.broker.listener.name=SASL\_PLAINTEXT**

* **Ý nghĩa**: Đây là tên của listener mà các broker khác trong cluster sẽ sử dụng để giao tiếp với nhau. Cần phải trùng với tên listener đã được định nghĩa trong advertised.listeners. Cấu hình này rất quan trọng để đảm bảo rằng các broker có thể kết nối với nhau một cách chính xác.

**4. sasl.mechanism.inter.broker.protocol=SCRAM-SHA-512**

* **Ý nghĩa**: Xác định cơ chế xác thực SASL mà các broker sẽ sử dụng khi giao tiếp với nhau. Trong trường hợp này, SCRAM-SHA-512 sẽ được sử dụng cho xác thực giữa các broker, giúp bảo mật hơn.

**5. listener.name.sasl\_plaintext.scram-sha-256.sasl.jaas.config=org.apache.kafka.common.security.scram.ScramLoginModule required username="admin" password="admin-secret";**

* **Ý nghĩa**: Đây là cấu hình JAAS cho listener SASL\_PLAINTEXT sử dụng cơ chế SCRAM-SHA-256. Cấu hình này cho biết rằng để kết nối qua listener này, một client cần cung cấp tên người dùng và mật khẩu. Trong trường hợp này, tên người dùng là admin và mật khẩu là admin-secret. Thông tin này được sử dụng để xác thực client khi nó cố gắng kết nối tới broker.

**6. sasl.enabled.mechanisms=SCRAM-SHA-256,SCRAM-SHA-512**

* **Ý nghĩa**: Danh sách các cơ chế SASL mà Kafka sẽ hỗ trợ cho client và broker. Ở đây, cả hai cơ chế SCRAM-SHA-256 và SCRAM-SHA-512 đều được phép sử dụng. Điều này có nghĩa là client có thể lựa chọn cơ chế nào mà nó hỗ trợ khi kết nối đến broker.

**Tổng kết**

Những cấu hình này đảm bảo rằng Kafka hoạt động với các kết nối bảo mật thông qua SASL, xác thực người dùng và thiết lập giao tiếp an toàn giữa các broker. Việc sử dụng SCRAM-SHA-512 giúp tăng cường mức độ bảo mật cho hệ thống, đặc biệt trong các môi trường nhạy cảm.