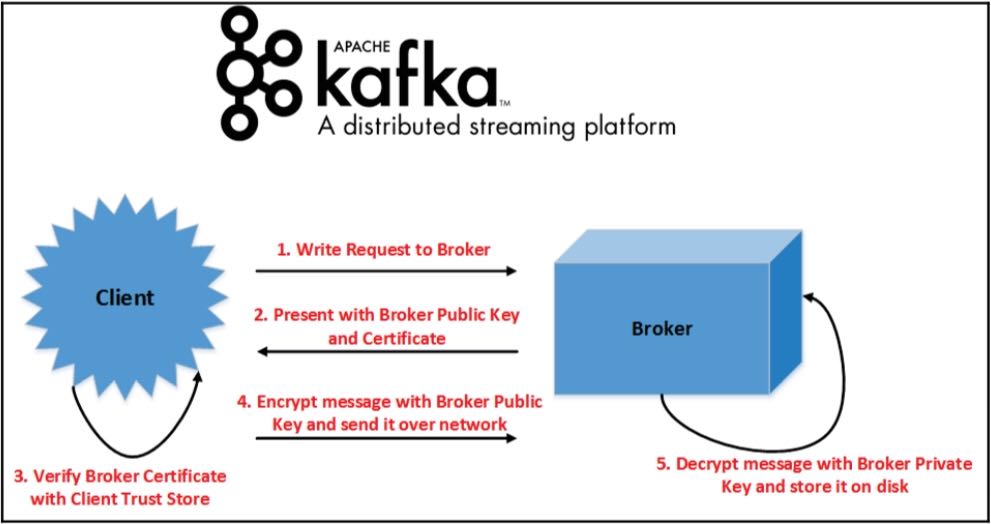
**Steps to enable SSL in Incubator Kafka**



The preceding diagram depicts how communication between broker and client is encrypted. This is valid for both producer and consumer communications. Every broker or client maintains their keys and certificates. They also maintain truststores containing certificates for authentication. Whenever certificates are presented for authentication, they are verified against certificates stored in truststores of respective components.

The incubator chart be updated to support SSL

configurationOverrides: {

"listeners": "PLAINTEXT://:9092,SSL://0.0.0.0:9091",

"ssl.client.auth": "required",

"ssl.truststore.location": "/var/run/secrets/kubernetes.io/serviceaccount/ca.crt",

"ssl.truststore.type": "PEM",

"ssl.keystore.location": "/opt/kafka/data/kafka-server.pfx",

"ssl.keystore.type": "PKCS12",

"ssl.keystore.password": "my-super-secure-secret"

}

**Creating SSL Keys and Certificates**

Configure all brokers in the Kafka cluster to accept secure connections from clients. Any configuration changes made to the broker will require a [rolling restart](https://docs.confluent.io/current/kafka/post-deployment.html#rolling-restart).

Enable security for Kafka brokers as described in the section below. Additionally, if you are using Confluent Control Center or Auto Data Balancer, configure your brokers for:

* [Confluent Metrics Reporter](https://docs.confluent.io/current/kafka/authentication_ssl.html#authentication-ssl-metrics-reporter)

1. Configure the truststore, keystore, and password in the server.properties file of every broker. Since this stores passwords directly in the broker configuration file, it is important to restrict access to these files via file system permissions.
2. ssl.truststore.location**=**/var/private/ssl/kafka.server.truststore.jks
3. ssl.truststore.password**=**test1234
4. ssl.keystore.location**=**/var/private/ssl/kafka.server.keystore.jks
5. ssl.keystore.password**=**test1234
6. ssl.key.password**=**test1234

Copy

Note: ssl.truststore.password is technically optional but highly recommended. If a password is not set, access to the truststore is still available, but integrity checking is disabled.

1. If you want to enable SSL for inter-broker communication, add the following to the broker properties file (it defaults to PLAINTEXT):
2. security.inter.broker.protocol**=**SSL

Copy

1. Configure the ports for the Kafka brokers to listen for client and inter-broker SSL connections. We need to configure listeners, and optionally advertised.listeners if the value is different from listeners.
2. listeners**=**SSL://kafka1:9093
3. advertised.listeners**=**SSL://0.0.0.0:9093

Copy

1. Configure both SSL ports and PLAINTEXT ports if:
   * SSL is not enabled for inter-broker communication
   * Some clients connecting to the cluster do not use SSL
2. listeners**=**PLAINTEXT://kafka1:9092,SSL://kafka1:9093
3. advertised.listeners**=**PLAINTEXT://0.0.0.0:9092,SSL://0.0.0.0:9093

Copy

*Note* that advertised.host.name and advertised.port configure a single PLAINTEXT port and are *incompatible* with secure protocols. Please use advertised.listeners instead.

1. To enable the broker to authenticate clients (2-way authentication), you need to configure all the brokers for client authentication. We recommend configuring this to required. (We discourage requested because misconfigured clients will still connect successfully and it provides a false sense of security)
2. ssl.client.auth**=**required

Copy

**Note**

If any of the SASL authentication mechanisms are enabled for a given listener, then SSL client authentication is disabled even if ssl.client.auth=required is configured, and the broker will authenticate clients only via SASL on that listener.

44-IPTUOBNFQ PSU 3. To give 44- keystore and truststores path for each broker, you should make the following changes in the server properties of each broker: TTMLFZTUPSFMPDBUJPO­QBUIUPLBGLBCSPLFSTFSWFSLFZTUPSFKLT TTMLFZTUPSFQBTTXPSE­LFZTUPSF@QBTTXPSE TTMLFZQBTTXPSE­LFZ@QBTTXPSE TTMUSVTUTUPSFMPDBUJPO­ QBUIUPLBGLBCSPLFSTFSWFSUSVTUTUPSFKLT TTMUSVTUTUPSFQBTTXPSE­USVTUTUPSF@QBTTXPSE Some other additional properties like security.inter.broker.protocol can also be used. Use the link IUUQTLBGLBBQBDIFPSHEPDVNFOUBUJPO TFDVSJUZ@DPOGJHCSPLFSfor additional properties.