Sentry Demo --- 2021 Jan 20

Step 1: Generating Keys and Certificates for Kafka Brokers

- Generate the key and the certificate for each machine in the cluster using the Java keytool utility.
- Make sure that the common name (CN) matches the fully qualified domain name (FQDN) of your server.
- The client compares the CN with the DNS domain name to ensure that it is connecting to the correct server.

Step 2: Creating Your Own Certificate Authority

- Certificate Authority is a genuine and trusted authority, the clients have high assurance that they are connecting to the authentic machines.

keytool -keystore {client.truststore.jks} -alias CARoot -import -file {ca-cert}

Step 3: Signing the Certificate

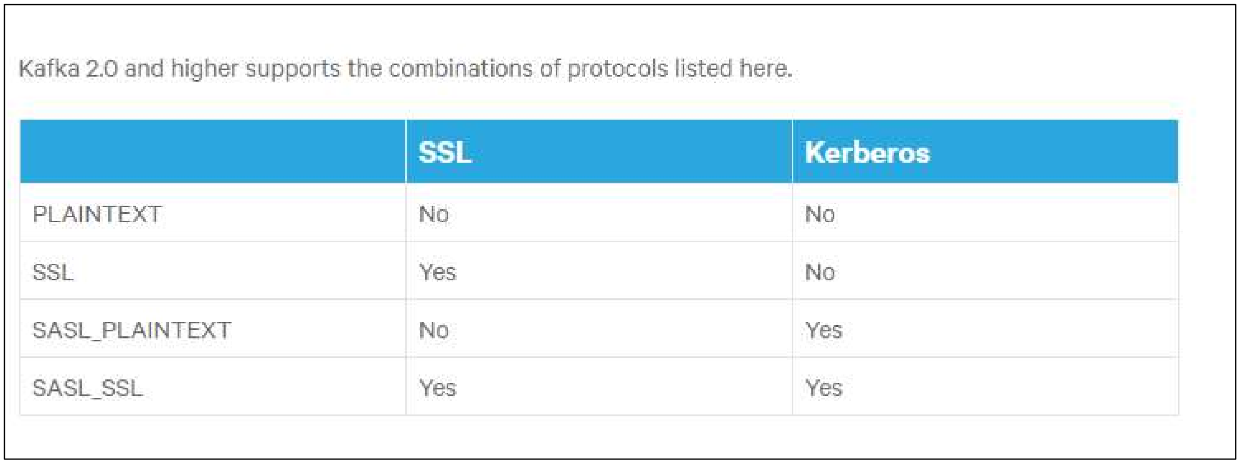
- Create a certificate request from the keystore : ***keytool -keystore server.keystore.jks -alias localhost -certreq -file cert-file***
- Sign the resulting certificate with the CA
- Import both the certificate of the CA and the signed certificate into the keystore

Step 4: Configuring Kafka Brokers

- Turn on SSL for the Kafka service by turning on the ssl_enabled configuration for the Kafka
- Set security.inter.broker.protocol as SSL, if Kerberos is disabled; otherwise, set it as SASL_SSL.

- **The following SSL configurations are required on each broker**. Each of these values can be set in Cloudera Manager.
- Be sure to replace this example with the truststore password.

- **ssl.keystore.location=/var/private/ssl/kafka.server.keystore.jks**
- **ssl.keystore.password=SamplePassword123**
- **ssl.key.password=SamplePassword123**
- **ssl.truststore.location=/var/private/ssl/server.truststore.jks**
- **ssl.truststore.password=SamplePassword123**



Kafka 2.0 and higher supports the combinations of protocols listed here.

	SSL	Kerberos
PLAINTEXT	No	No
SSL	Yes	No
SASL_PLAINTEXT	No	Yes
SASL_SSL	Yes	Yes

Topic Authorization with Kerberos and Sentry

Configuring Kafka to Use Sentry Authorization

The following steps describe how to configure Kafka to use Sentry authorization

- **Granting Privileges to a Role**
  - Create Role : **kafka-sentry -cr -r test**
  - To confirm that the role was created: **kafka-sentry -lr**

  - Allow users in **testGroup** to write to **testTopic** from **localhost**, which allows users to produce to testTopic. Users need both write and describe permissions.
    Grant the create privilege to the test role:

    kafka-sentry -gpr -r test -p "Host=127.0.0.1->Topic=testTopic->action=write"
    kafka-sentry -gpr -r test -p "Host=127.0.0.1->Topic=testTopic->action=describe"

- Assign the test role to the group testGroup : **kafka-sentry -arg -r test -g testGroup**

- Allow users in **testGroup** to read from a **consumer group, testconsumergroup**
- Verify that the test role is part of the group testGroup : **kafka-sentry -lr -g testGroup**

Troubleshooting Kafka with Sentry

/var/log/kafka/kafka-broker-host-name.log

Designed by Wikasitha Herath