Scenario 6

Problem-statement :

The client just performed a lift and shift on their entire platform to different machines. The brokers and several other components are down.
The brokers have the following error log -

Observation :

When I run docker-compose up -d then I observed that kafka1, kafka2, kafka3 and connector was down .

Errors :

1. java.lang.RuntimeException: Received a fatal error while waiting for all of the authorizer futures to be completed.

at kafka.server.KafkaServer.startup(KafkaServer.scala:950)
at kafka.Kafka$.main(Kafka.scala:114)
at kafka.Kafka.main(Kafka.scala)
Caused by: java.util.concurrent.CompletionException: org.apache.kafka.common.errors.SslAuthenticationException: SSL handshake failed
at java.base/java.util.concurrent.CompletableFuture.encodeRelay(CompletableFuture.java:367)
at java.base/java.util.concurrent.CompletableFuture.completeRelay(CompletableFuture.java:376)
at java.base/java.util.concurrent.CompletableFuture$AnyOf.tryFire(CompletableFuture.java:1663)
at java.base/java.util.concurrent.CompletableFuture.postComplete(CompletableFuture.java:506)
at

2. For second error after the resolve of above error i am geting another issue with metrics is not visually representing in the control-center

Aproach / Method :

TLS AND MTLS (renewal of certificates) &&
valid configuration superuser names for kafkabrokers and broker.users in kafka brokers
Change the certificate CN name on each kafka broker by updating the certificates of every broker

Detailed Solution :

1. **Renewal of certificates** :

While I up the docker-compose first I observed the kafka-brokers are down and then I logged the each containers then I have got the ssl certificate errors .then I have checked the certificate validities and passwords and correct paths and matched . I pointed out that error was due to certificate validity they have expired .
Then I have renewed the certificates of all brokers by using commands
Commands :

keytool -keystore kafka.server.keystore.jks -alias localhost -certreq -file kafka-broker-new.csr

openssl x509 -req -CA ~/tasks/cp-sandbox/certs/ca-cert -CAkey ~/tasks/cp-sandbox/certs/ca-key -in kafka-broker-new.csr -out kafka-broker-new-signed-cert.pem -days 365 -CAcreateserial

keytool -keystore kafka.server.keystore.jks -alias localhost -import -file kafka-broker-new-signed-cert.pem

Again then I have checked the certificates and then watched the validate the expiry date its good and updated for 365 days.

2. **Adding configuration to disable hostname verification :**

Add the configuration to all server.properties of kafka brokers (kafka1, kafka2, kafka3)

Ssl.endpoint.identification.algorithm= <null> or “”

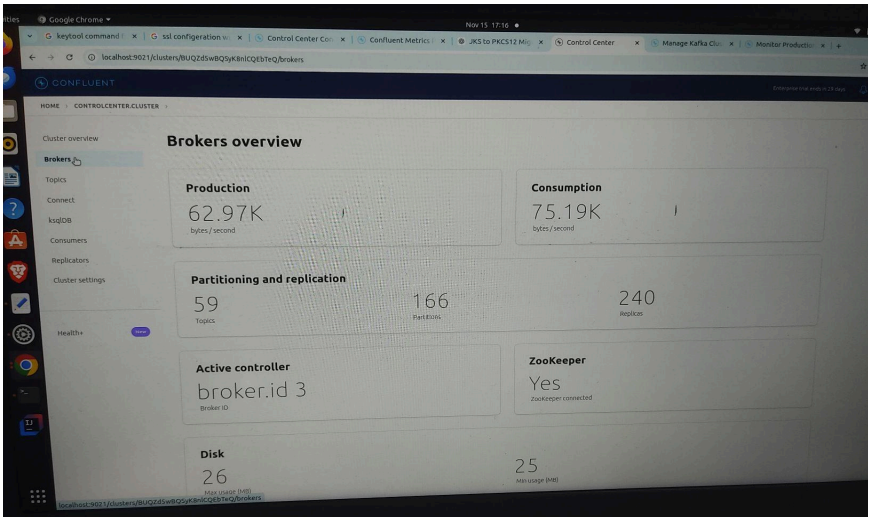
Here we are setting the above config to null means empty or set as empty string to disable the hostname verification for kafka brokers

3. **Disable hostname verification for confluent metrsics**

Add below configs to kafka brokers

Confluent.metrics.ssl.endpoint.identification.algorithm = <null> or “”

Here we are setting the above config to null means empty or set as empty string to disable the hostname verification for confluent-center to vissualize the metrics like production and cunsumptions



Conclusion :

- [ ] If we get certification validation issue renew the certificates
- [ ] If we get ssl handshake failed due to authorization then disable the hostname verification or check the usernames for brokers
- [ ] If the broker metrics are not visually representing in the control-center make sure that hostname verifications if the hostnames and usernames are different disable the hostname verification