scenario6

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 and schema registry was down . And after the solving the kafka brokers and other component down issues like ssl handshake

Errors :

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

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 correct valid super.user and bootstrap.users :**

   Add correct super.users for kafka brokers replace the

   - Kafka-1 >>>> kafka1
   - Kafka-2 >>>> kafka2
   - Kafka-3 >>>> kafka3

   Same for broker..user replace it by the above values

3. **Update the certificates again by changing the CN name for all kafka brokers :**
   Use below commands to update your certificates

   COMMANDS :

   keytool -keystore kafka.server.keystore.jks -alias localhost -certreq -file kafka-broker-new.csr -dnames “CN=kafka-1, OU=training, O=Platformatory, L=Bengaluru, ST=Karnataka, C=IN”

   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
   Update the CN names by by adding correct names

Conclusion :

- ☐ We we got error like ssl handshake failed first we need to check the correct keystore names and check paths mentioned for those files and then check for passwords for their files.

- [ ] Then move to super.users and broker.user names they
- [ ] Finally check and match these names to respected certificates names (CN names) and if they are not match update the certificates
- [ ] Then again run the docker-compose file