

Scenario 9

Problem-statement :

The client just upgraded their SSL certificates used for the inter broker communication. The cluster was healthy before the certificate updates. After the certificate updates, the client sees the following error in the broker logs -

Observation :

Brokers are down and connect ,control-center, schema-registry are also down. I have checked the logs and found the `_confluent-metadata-auth` not authorized

Errors :

1. Caused by: java.util.concurrent.CompletionException:
org.apache.kafka.common.errors.TopicAuthorizationException: Not authorized to
access topics: [_confluent-metadata-auth] 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
java.base/java.util.concurrent.CompletableFuture.completeExceptionally(CompletableFuture.java:2088) at
io.confluent.security.auth.provider.ConfluentProvider.lambda\$null\$10(ConfluentProvider.java:543)at
java.base/java.util.concurrent.CompletableFuture.uniExceptionally(CompletableFuture

Approach / Method :

TLS (renewal of certificates) &&
valid configuration superuser names for kafkabrokers and broker.users in kafka
brokers
Check for certificates of cn names and validates with it to ssl settings in
server.properties

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. Updating the mapping rules in kafka broker server.properties :

The error indicates brokers are down due to the authorization errors to the _confluent-metdata-auth topic

So we need to check the certificates first of each brokers and find out the cn names for the certificates then check the ssl settings super.users, broker.users and check the weather ssl.endpoint.identification.algorithm is set to empty

This is used for hostname verification disable

After checking all the properties

```
Super.users  
Broker.users  
Certificates cn names  
Ssl.endpoint.identification.algorithm
```

Although I am getting same error

Then I moved to server.properties and looked for the mapping rules

- Ssl.principle.mapping.rules =
RULE:^.*CN=([a-zA-Z0-9]*),.*\$/\$1/L,DEFAULT

This rule is for kafka1, kafka2, kafka3 cn names

Changed to >>>>>>

- ssl.principal.mapping.rules=RULE:^.*CN=([a-z]*[-][0-9]),.*\$/\$1/L,DEFAULT

This rule is for the kafka-1, kafka-2, kafka-3 cn names due to certificate . set it to all 3 broker's server.properties

Conclusion :

- ☐ Check the kafka brokers certificate validity and then renewal if certificate's validity would have expired
- ☐ If we get authorization error of internal topics check the super.users Broker.users and validate the certificate cn names with the hostnames And then check for correct ssl settings