**REFERENCE:** <https://comviva.atlassian.net/wiki/spaces/MOB/pages/268468237/Kafka+with+SASL_SSL>

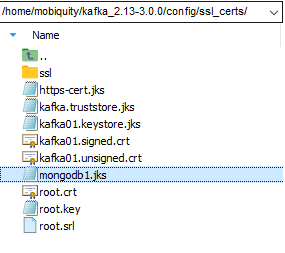
CA signed certificates and JKS are used

The JKS file contains all intermediate, root, server certificate and private key

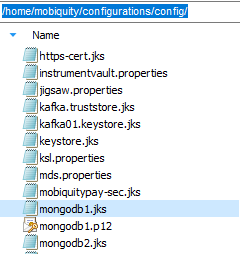
sudo openssl pkcs12 -export -in mongodb.pem -out mongodb1.p12

sudo keytool -importkeystore -srckeystore mongodb1.p12 -srcstoretype PKCS12 -destkeystore mongodb1.jks -deststoretype JKS

For kafka server



For client



**cat /etc/hosts**

127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4

::1 localhost localhost.localdomain localhost6 localhost6.localdomain6

172.25.48.30 svc-eig eighost svc-token svc-mongodb svc-couchdb svc-influxdb svc-repo svc-rp svc-pentaho svc-elasticdb svc-vault svc-rabbitmq1 svc-kafka svc-schema svc-kafka1 svc-bulk svc-redis svc-host dfs-mobiquitypay-security-application-server svc-config-server svc-mongodb.comviva.com svc-valkey dfssecmobiquity.comviva.com krakend-test.comviva.com svc-krakend **svc-kafka.comviva.com**

172.25.48.86 svc-oracle svc-postgre oracle-db-host svc-postgres svc-postgres-reporting svc-oracle-reporting

172.25.49.169 svc-lb krakend.comviva.com ui-host jigsaw.comviva.com dms.comviva.com

**KAFKA side configurations**

Follow these steps one by one to make changes in properties and service file

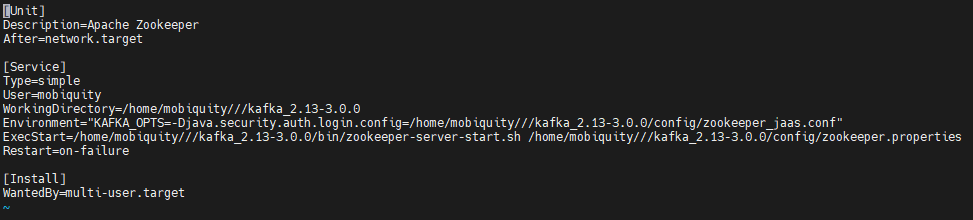
1. sudo systemctl stop kafka
2. sudo systemctl stop zookeeper
3. sudo vi /home/mobiquity/kafka\_2.13-3.0.0/config/zookeeper.properties

Ensure these properties are present there:

authProvider.1=org.apache.zookeeper.server.auth.SASLAuthenticationProvider  
requireClientAuthScheme=sasl  
If these are already present, no further changes are required.

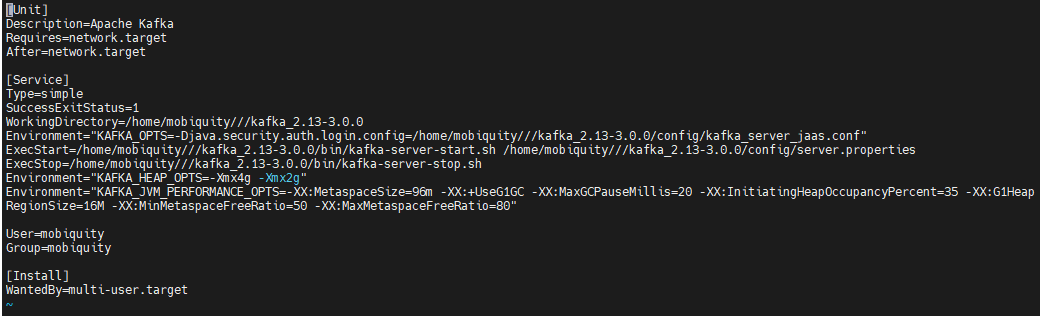
1. sudo vi /home/mobiquity/kafka\_2.13-3.0.0/config/zookeeper\_jass.conf  
   Ensure server{} config is there.   
   If present, no changes to be done. Here note that server{} will contain some username and passwords.
2. sudo vi /home/mobiquity/kafka\_2.13-3.0.0/config/kafka\_server\_jaas.conf  
   Ensure kafkaserver{} config and client{} config is there.   
   If present, no changes to be done. Here, note that server{} and client{} config will contain some username and passwords.
3. sudo vi /etc/systemd/system/zookeeper.service  
   Add the following command in [service]:

Environment="KAFKA\_OPTS=-Djava.security.auth.login.config=/home/mobiquity///kafka\_2.13-3.0.0/config/zookeeper\_jaas.conf"  
  
This is how final zookeeper.service should look like:



1. sudo vi /etc/systemd/system/kafka.service  
   Add the following command in [service]:

Environment="KAFKA\_OPTS=-Djava.security.auth.login.config=/home/mobiquity///kafka\_2.13-3.0.0/config/kafka\_server\_jaas.conf"  
  
This is how final kafka.service should look like:



1. sudo systemctl daemon-reload
2. sudo vi /home/mobiquity/kafka\_2.13-3.0.0/config/server.properties

zookeeper.connect=**svc-kafka.comviva.com**

# #AUTH

#security.inter.broker.protocol=SASL\_PLAINTEXT

#sasl.mechanism.inter.broker.protocol=PLAIN

#sasl.mechanism=PLAIN

#sasl.enabled.mechanisms=PLAIN,METADATA

#security.protocol=SASL\_PLAINTEXT #authorizer.class.name=kafka.security.auth.SimpleAclAuthorizer #authorizer.class.name=kafka.security.authorizer.AclAuthorizer #allow.everyone.if.no.acl.found=true

#listeners=SASL\_PLAINTEXT://0.0.0.0:9092 #advertised.listeners=SASL\_PLAINTEXT://172.25.48.30:9092

#host.name=172.25.48.30

#ssl changes

listeners=SASL\_SSL://svc-kafka.comviva.com:9092

advertised.listeners=SASL\_SSL://svc-kafka.comviva.com:9092

ssl.truststore.location=/home/mobiquity/kafka\_2.13-3.0.0/config/ssl\_certs/mongodb1.jks ssl.truststore.password=mobiquity

ssl.keystore.location=/home/mobiquity/kafka\_2.13-3.0.0/config/ssl\_certs/mongodb1.jks ssl.keystore.password=mobiquity

ssl.key.password=mobiquity

ssl.enabled.protocols=TLSv1.2,TLSv1.3,TLSv1,TLSv1.1 listener.name.saslSSL.ssl.client.auth=required

ssl.keystore.type=JKS

ssl.truststore.type=JKS

ssl.endpoint.identification.algorithm=

security.inter.broker.protocol=SASL\_SSL

sasl.enabled.mechanisms=PLAIN

sasl.mechanism.inter.broker.protocol=PLAIN authorizer.class.name=kafka.security.authorizer.AclAuthorizer allow.everyone.if.no.acl.found=true

auto.create.topics.enable=false

1. sudo vi /home/mobiquity/kafka\_2.13-3.0.0/config/consumer.properties

#bootstrap.servers=localhost:9092

#security.protocol=SASL\_PLAINTEXT

security.protocol=SASL\_SSL

bootstrap.servers=svc-kafka.comviva.com:9092

ssl.endpoint.identification.algorithm= ssl.truststore.location=/home/mobiquity/kafka\_2.13-3.0.0/config/ssl\_certs/mongodb1.jks ssl.truststore.password=mobiquity

ssl.keystore.location=/home/mobiquity/kafka\_2.13-3.0.0/config/ssl\_certs/mongodb1.jks ssl.keystore.password=mobiquity

ssl.key.password=mobiquity

1. sudo vi /home/mobiquity/kafka\_2.13-3.0.0/config/producer.properties

#bootstrap.servers=172.25.48.30:9092

#security.protocol=SASL\_PLAINTEXT

security.protocol=SASL\_SSL

bootstrap.servers=svc-kafka.comviva.com:9092

ssl.truststore.location=/home/mobiquity/kafka\_2.13-3.0.0/config/ssl\_certs/mongodb1.jks ssl.truststore.password=mobiquity

ssl.keystore.location=/home/mobiquity/kafka\_2.13-3.0.0/config/ssl\_certs/mongodb1.jks ssl.keystore.password=mobiquity

ssl.key.password=mobiquity

ssl.endpoint.identification.algorithm=

1. sudo systemctl start zookeeper
2. sudo systemctl start kafka

Follow these 12 steps and your kafka will be sasl\_ssl ready.

## **Client Side Changes:**

1. **SOE.properties**

#Kafka configuration

#kafka.bootstrap-servers=svc-kafka1:9092

#kafka.audit.bootstrap-servers=svc-kafka1:9092

#kafka.ip.ports=svc-kafka1:9092

#security.protocol=SASL\_PLAINTEXT

#sasl.mechanism=PLAIN

#outstream.kafka.ip.ports=svc-kafka1:9092

outstream.kafka.ip.ports=svc-kafka.comviva.com:9092

kafka.bootstrap-servers=svc-kafka.comviva.com:9092

kafka.audit.bootstrap-servers=svc-kafka.comviva.com:9092

kafka.ip.ports=svc-kafka.comviva.com:9092

BOOTSTRAP\_SERVERS\_CONFIG=svc-kafka.comviva.com:9092 security.protocol=SASL\_SSL

sasl.mechanism=PLAIN ssl.truststore.location=/home/mobiquity/configurations/config/mongodb1.jks ssl.truststore.password=mobiquity ssl.keystore.location=/home/mobiquity/configurations/config/mongodb1.jks ssl.keystore.password=mobiquity

ssl.key.password=mobiquity

ssl.endpoint.identification.algorithm= ssl.enabled=true

Along with this code level changes

And Restart SOE

1. **Notification Producer**

#kafka.bootstrap-servers=svc-kafka1:9092

#security.protocol=SASL\_PLAINTEXT

#sasl.mechanism=PLAIN

kafka.bootstrap-servers=svc-kafka.comviva.com:9092 BOOTSTRAP\_SERVERS\_CONFIG=svc-kafka.comviva.com:9092 security.protocol=SASL\_SSL

sasl.mechanism=PLAIN ssl.truststore.location=/home/mobiquity/configurations/config/mongodb1.jks ssl.truststore.password=mobiquity ssl.keystore.location=/home/mobiquity/configurations/config/mongodb1.jks ssl.keystore.password=mobiquity

ssl.key.password=mobiquity

ssl.endpoint.identification.algorithm=

ssl.enabled=true

1. **Notification Consumer**

#kafka.bootstrap-servers=svc-kafka1:9092

#security.protocol=SASL\_PLAINTEXT

#sasl.mechanism=PLAIN

kafka.bootstrap-servers=svc-kafka.comviva.com:9092 BOOTSTRAP\_SERVERS\_CONFIG=svc-kafka.comviva.com:9092 security.protocol=SASL\_SSL

sasl.mechanism=PLAIN ssl.truststore.location=/home/mobiquity/configurations/config/mongodb1.jks ssl.truststore.password=mobiquity ssl.keystore.location=/home/mobiquity/configurations/config/mongodb1.jks ssl.keystore.password=mobiquity

ssl.key.password=mobiquity

ssl.endpoint.identification.algorithm=

ssl.enabled=true

Along with this code level changes

And Restart notification P C

1. **Buds.properties**

#kafka.bootstrap-servers=svc-kafka1:9092

#security.protocol=SASL\_PLAINTEXT

#sasl.mechanism=PLAIN

kafka.bootstrap-servers=svc-kafka.comviva.com:9092 BOOTSTRAP\_SERVERS\_CONFIG=svc-kafka.comviva.com:9092 security.protocol=SASL\_SSL

sasl.mechanism=PLAIN ssl.truststore.location=/home/mobiquity/configurations/config/mongodb1.jks ssl.truststore.password=mobiquity ssl.keystore.location=/home/mobiquity/configurations/config/mongodb1.jks ssl.keystore.password=mobiquity

ssl.key.password=mobiquity

ssl.endpoint.identification.algorithm=

ssl.enabled=true

1. **KSL.properties**

#kafka.bootstrap-servers=svc-kafka1:9092

#security.protocol=SASL\_PLAINTEXT

#sasl.mechanism=PLAIN

kafka.bootstrap-servers=svc-kafka.comviva.com:9092 BOOTSTRAP\_SERVERS\_CONFIG=svc-kafka.comviva.com:9092 security.protocol=SASL\_SSL

sasl.mechanism=PLAIN ssl.truststore.location=/home/mobiquity/configurations/config/mongodb1.jks ssl.truststore.password=mobiquity ssl.keystore.location=/home/mobiquity/configurations/config/mongodb1.jks ssl.keystore.password=mobiquity

ssl.key.password=mobiquity

ssl.endpoint.identification.algorithm= ssl.enabled=true

1. **Kafka connect**

sudo vi /home/mobiquity/kafka\_2.13-3.8.1/config/connect-distributed.properties

#bootstrap.servers=svc-kafka1:9092

bootstrap.servers=svc-kafka.comviva.com:9092

#security.protocol=SASL\_PLAINTEXT

security.protocol=SASL\_SSL

#producer.security.protocol=SASL\_PLAINTEXT

producer.security.protocol=SASL\_SSL

#consumer.security.protocol=SASL\_PLAINTEXT

consumer.security.protocol=SASL\_SSL