**Kafka Authentication and authorization using SSL/TLS**

1. Generate public & private key pairs for client and server
2. Configure server to accept secure connection over SSL
3. Enable client authentication using SSL certificate
4. Setup ACLs on Kafka topics
5. Online resource
6. Setup Zookeeper security (Incomplete. Admins to complete this step)
7. Kafka security documentation: <https://kafka.apache.org/documentation/#security>
8. **Generate public & private key pairs for client and server**
9. Generate JKS keystore for client and server
10. Exchange public certs between client and server keystores
11. At this point, server keystore will have server private & public key and client public key. Client keystore will have client private & public keys and server public key.
12. If you have multi-broker cluster and you intend to use different keystore for each broker, you should do public key exchange among broker keystores.

Pending: scripts to automate generate and exchange of public keys

1. **Configure Kafka server to accept secure connection over SSL**
2. Add below settings into server.properties (modify ports and paths as needed)

**listeners= SSL://:9492**

**security.inter.broker.protocol=SSL**

**allow.everyone.if.no.acl.found=false**

**ssl.keystore.location=I:/eh/ssl/kafka\_local/server1.keystore.jks**

**ssl.keystore.password=password1**

**ssl.key.password=password1**

**ssl.truststore.location=I:/eh/ssl/kafka\_local/server1.keystore.jks**

**ssl.truststore.password=password1**

**authorizer.class.name=kafka.security.auth.SimpleAclAuthorizer**

**super.users=User:CN=server1,OU=localkafka,O=jpmchase,C=US;User:CN=server2,OU=localkafka,O=jpmchase,C=US;User:CN=server3,OU=localkafka,O=jpmchase,C=US**

1. **Enable client authentication using SSL certificate**
   1. After step-2,client and server can communicate over SSL, but client still don’t need to authenticate to server
   2. Enable client authentication using SSL. This setting forces client to provide valid SSL cert issued to client that server can recognize.

**ssl.client.auth=required**

1. **Setup ACLs on Kafka topics. ACLs will authorize which client has what level of access** 
   1. Use below command to setup ACLs on each topic for particular client.
      1. Allow putting messages to topic for user CN=client2

Kafka-acls.bat –authorizer-properties zookeeper.connect=localhost:2181 –add –allow-principal User:CN=client1, OU=JPM,C=US --produce–topic <topicname>

* + 1. Allow getting messages from topic for user CN=client1

Kafka-acls.bat –authorizer-properties zookeeper.connect=localhost:2181 –add –allow-principal User:CN=client1, OU=JPM,C=US --consume –topic <topicname>

* + 1. You can also get fine grain control using other options to kafka-acls command.

1. **For more details instructions on various authentication methods**

<https://kafka.apache.org/documentation/#security>

1. **Setup Zookeeper security**
   1. Add below settings to zookeeper.properties

authProvider.1 = org.apache.zookeeper.server.auth.SASLAuthenticationProvider

requireClientAuthScheme=sasl

jaasLoginRenew=3600000

* 1. Setup zookeeper.server.jaas.conf file

Server {

org.apache.zookeeper.server.auth.DigestLoginModule required

user\_admin="adminsecret"

user\_broker="password1";

};

};

* 1. Zookeeper now should only allow connections from those users that are added to above conf file.