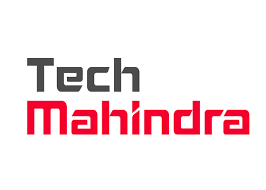
DAAIP Kafka Interface for Clients

Strictly Confidential

1. Add the following Kafka broker IP address in the /etc/hosts, as we are using SSL , kafka broker will be identified by host name

10.224.156.4 KAFKA1-PROD-S1

10.224.156.5 KAFKA2-PROD-S3

10.224.156.6 KAFKA3-PROD-S4

1. Use the shared truststore file and the password(will be shared separately) for consuming DAAIP Kafka brokers (KAFKA1-PROD-S1, KAFKA2-PROD-S3, KAFKA3-PROD-S4). it has all the three broker certificates
2. The following property file will be used while running the kafka consumer command from the command prompt



**Note** – Copy the client-ssl.properties file in the kafka config folder

Content of **client-ssl.properties** file is copied below. Replace the highlighted yellow color with the exact location of the truststore file (kafka.client.truststore.jks) in your system,and the truststore password(will be shared separately)

security.protocol=SSL

bootstrap.servers=KAFKA1-PROD-S1:9093,KAFKA2-PROD-S3:9093,KAFKA3-PROD-S4:9093

ssl.truststore.location=/home/daaip/ssl/kafka.client.truststore.jks

ssl.truststore.password=password

1. As Kafka client , the following command can be run from the command prompt

./bin/kafka-console-consumer.sh --bootstrap-server KAFKA1-PROD-S1:9093 --topic AlarmSync1 --consumer.config ./config/client-ssl.properties

1. Port – 9093
2. Retention period – 4 days
3. List of topic names

* AlarmSync1
* AlarmSync2
* AlarmSync3
* AlarmSync4