Broker Config

The important configurations are the following:

- broker. id
- log. dirs
- zookeeper. connect

Property	Description
broker.id	It is a list of a lot of directories arranged properly separated by commas and each partition is placed in the directory having the less number of partitions.
log.dirs	It stores the log and used when it is 0.
zookeeper.connect	ZK leader and follower distance

Name	Explanation
bootstrap. servers	A list of host/port pairs to use in establishing the initial connection to the Kafka cluster.It initiates the total servers.
key. serializer	It is the key to implement the interface for the serializer
value. serializer	It is the value for the same
acks	When it is 0, the producer asks for no acknowledgement. If 1, the leader will acknowledge without the concern of other followers. When act=all, until all the in-sync replicas are acknowledged, the leader will wait for approving it. It gives full guarantee.
Buffer. memory	The total memory is buffered before sending.If all the blocks are sent together, then the producer will block or

	buffer it so that delivery to the server do not overlap. Buffering uses only a part of the memory not all. Few parts of memory are for compressing and other requests.
compression. type	It tells about the compressing of data made by the producer. It compresses the full set of data so compression is of higher quality. If more batching is done.it automatically qualifies the compression. Gzip and snappy are valid.
retries	If transfer of any record fails, then the client sends it again if retries is set to 1.Using this, the user has to be careful, because, if the producer sends two data together and if one is failed and we retry sending it. In that case the first one will get delivered after the second one.
ssl.key.password	Its password is for storing the files with a key.
ssl.keystore.location	It tells about the location whey the file is stored.
ssl.keystore.password	It is the password for the store of the key store file.it required only when location key is used
ssl.truststore.location	It gives the location of the file used to store the trust.
ssl.truststore.password	The password for the trust store file.
batch.size	If a lot of records are needed to accumulate together, the producer attempts for fewer number of the records so that it assists the performance of servers as well as for the clients. Sizes are trying to be minimized as possible. Batch sizes should be proper because if it is smaller than it may affect the throughput. And if the size is more than required, then it will waste a lot of its memory.
client.id	Its an id to use for making requests to the broker. It is sent to the servers so that they allows to track the source of requests.
connections.max.idle.ms	If the given time is expired, it shuts down the connections so that no extra time is beg wasted.
max.block.ms	Sometimes memory becomes full or unavailable. So at that time, the links need to be blocked so that data do not overflow.
max.request.size	It indicates till what size, you can make the request and also how big your record can be. The request the producer does should not exceed the maximum limit and this command have to make sure of it.
partitioner.class	This is a class that implements the interface of the partitioner.

receive.buffer.bytes	It indicates the size of the buffer that is used to read the records and requests.
request.timeout.ms	If any request takes more time to reach the customer, then the customer can stop it by this command.If the record or request fails and still there is time, then the customer will wait and the we can resend it.
sasl.kerberos.service.name	It dictates how the Kafka tool runs in the JAAS configuration.
security.protocol	These are some security rules and regulations used while exchanging words with the servers.
send.buffer.bytes	It indicates the size of the memory buffer which will hold the data to be sent to the producer.
ssl.enabled.protocols	It is the lists of the rules for maintaining the connections related to SSL.
ssl.keystore.type	It is not the key, but the format of how the key should be.
ssl.protocol	It is responsible for the contexts. TLS is the original one and, TLSv1.1 and TLSv1.2. SSL, SSLv2 are for other virtual machines.
ssl.provider	It provides security for the virtual machine. And its name and value will be similar to the security giver of the virtual machine.
ssl.truststore.type	It indicates the file formation of the trust stores.
timeout.ms	It tells the maximum time the brokers wait for the requests. If the time is exceededthen it is set to one and block the request from reaching the servers. If the timeout is not one even if the time is exceeded, there an error will be elapsed.
metadata.fetch.timeout.ms	When time is out or memory overflows, so accepting of additional data needs to be stopped either by blocking or by showing errors. Sometimes when blocking is not urgent, you can show errors just by resetting this to zero.
metadata.max.age.ms	Prior to sending data, it studies about the meta data of the Topic to find out which broker serves the host. So ones the meta data of the Topic and its host is calculated, accordingly you can send data to the Topic.
metric.reporters	It contains classes that are used as reporters and by using those reporters, allows using classes for creating new metrics.

metrics.num.samples	It indicates the quantity of the samples for the metrics creation.
metrics.sample.window.ms	It indicates the quantity of the samples for the metrics creation.
reconnect.backoff.ms	Establishing reconnection to any host needs time and it is specified by this command. It makes the bond with the hosts stronger.
retry.backoff.ms	The amount of time to wait before attempting to retry a failed fetch request to a given Topic partition
sasl.kerberos.min.time.before.relogin	These are logged in and logout timings between the refreshing.
sasl.kerberos.ticket.renew.jitter	During the renewal period certain jitter is added and this jitter is calculated in percentage by this command.
sasl.kerberos.ticket.renew.window.factor	Until the next renewal of ticket is raised the login thread will be silent.
ssl.cipher.suites	For negotiating the network connection with TLS, the group of algorithms for encrypting and authority are in this list. All the suites included in this list is supported.
ssl.endpoint.identification.algorithm	It validates the server hostname
ssl.keymanager.algorithm	It is used for the SSL connection maintenance.
ssl.trustmanager.algorithm	Even it is for the connection maintenance used by trust manager. Its value is similar to the trust manager's value in the virtual machine.

delete.topic.enable=true