[**Install Kafka Cluster(Kraft) with SASL\_PLAINTEXT and ACL configs**](https://confluence.kapitalbank.az/display/DPS/Install+Kafka+Cluster%28Kraft%29+with+SASL_PLAINTEXT+and+ACL+configs)

Kafka version: 3.5.1  
OS: Rhel 8

Update OS and Install Java 11:

yum update  
yum install java-11-openjdk.x86\_64

Download and move to permanent folder Kafka:

wget https://downloads.apache.org/kafka/3.5.1/kafka\_2.13-3.5.1.tgz  
tar -xvf kafka\_2.13–3.5.1.tgz  
mv kafka\_2.13–3.5.1 kafka  
mv kafka /opt

Configure Kafka with Kraft:

sed -i s/^SELINUX=.\*$/SELINUX=disabled/ /etc/selinux/config  
  
setenforce 0  
  
systemctl disable — now firewalld  
  
mkdir /opt/kafka/data  
  
mkdir /opt/kafka/logs\_metadata  
  
cd /opt/kafka/config/kraft/  
  
mv server.properties server.properties.org  
  
vim server.properties   
  
# Warning. node.id will be different. Example: node.id=1 on the server1, node.id=2 on the server 2 etc.  
#########################  
   
node.id=1  
num.network.threads=3  
num.io.threads=8  
log.dirs=/opt/kafka/data  
metadata.log.dir=/opt/kafka/logs\_metadata  
   
   
process.roles=broker,controller  
listeners=BROKER://serverip:9092,CONTROLLER://serverip:9093  
advertised.listeners=BROKER://serverip:9092  
listener.security.protocol.map=BROKER:SASL\_PLAINTEXT,CONTROLLER:SASL\_PLAINTEXT  
controller.quorum.voters=1@server1ip:9093,2@server2ip:9093,3@server3ip:9093  
   
inter.broker.listener.name=BROKER  
controller.listener.names=CONTROLLER  
   
sasl.enabled.mechanisms=PLAIN  
sasl.mechanism.controller.protocol=PLAIN  
sasl.mechanism.inter.broker.protocol=PLAIN  
   
authorizer.class.name=org.apache.kafka.metadata.authorizer.StandardAuthorizer  
allow.everyone.if.no.acl.found=false  
super.users=User:admin  
   
delete.topic.enable=true  
socket.send.buffer.bytes=1048576  
socket.receive.buffer.bytes=1048576  
socket.request.max.bytes=104857600  
   
num.partitions=3  
default.replication.factor=2  
min.insync.replicas=2  
log.retention.hours=168  
log.segment.bytes=1073741824  
log.retention.check.interval.ms=300000  
auto.create.topics.enable=true  
unclean.leader.election.enable=false  
   
############################

Generate Kafka cluster ID:

bash /opt/kafka/bin/kafka-storage.sh random-uuid

Use the same Kafka cluster ID on each node:

bash /opt/kafka/bin/kafka-storage.sh format -t GeneratedUUID -c /opt/kafka/config/kraft/server.properties

Configure JAAS file. This file is for cluster authentication. Also, users will be configured on this file:

vim /opt/kafka/config/kraft/jaas.config  
   
KafkaServer {  
 org.apache.kafka.common.security.plain.PlainLoginModule required  
 username="admin"  
 password="admin"  
 user\_admin="admin"  
 user\_usera="usera"  
 user\_userb="userb";  
};

Create a config file for maintenance Kafka brokers. Because also server admins cannot do anything without authentication: (Create new topic,ACL etc..)

vi /opt/kafka/config/kraft/admin.config  
   
sasl.jaas.config=org.apache.kafka.common.security.plain.PlainLoginModule required username="admin" password="admin";  
security.protocol=SASL\_PLAINTEXT  
sasl.mechanism=PLAIN

Create Kafka service:

vim /etc/systemd/system/kafka.service  
   
[Unit]  
Description=kafka Service  
After=network-online.target  
Requires=network-online.target  
   
[Service]  
   
Type=simple  
Restart=on-failure  
  
User=root  
Group=root  
SyslogIdentifier=kafka  
Environment="KAFKA\_HEAP\_OPTS=-Xms1G -Xmx1G"  
Environment="KAFKA\_OPTS=-Djava.security.auth.login.config=/opt/kafka/config/kraft/jaas.config"  
   
ExecStart=/opt/kafka/bin/kafka-server-start.sh /opt/kafka/config/kraft/server.properties  
ExecStop=/opt/kafka/bin/kafka-server-stop.sh /opt/kafka/config/kraft/server.properties  
WorkingDirectory=/opt/kafka  
   
[Install]  
WantedBy=multi-user.target

Start and enable Kafka service:

systemctl daemon-reload  
   
systemctl enable --now kafka

Create Kafka Topic:

bash /opt/kafka/bin/kafka-topics.sh — bootstrap-server serverip:9092 — create — topic newtopic — partitions 2 — replication-factor 2 — command-config /opt/kafka/config/kraft/admin.config

Grant access to user for topic: (Operation can be: All,Read,Write etc..)

bash /opt/kafka/bin/kafka-acls.sh — bootstrap-server serverip:9092 — command-config /opt/kafka/config/kraft/admin.config — add — allow-principal User:usera — operation All — topic newtopic

Remove access of user from topic:

bash /opt/kafka/bin/kafka-acls.sh — bootstrap-server serverip:9092 — command-config /opt/kafka/config/kraft/admin.config — remove — allow-principal User:usera — operation Write — topic newtopic

Grant access to user for read from consumer group:

bash /opt/kafka/bin/kafka-acls.sh — bootstrap-server serverip:9092 — command-config /opt/kafka/config/kraft/admin.config — add — allow-principal User:admin — operation All— topic newtopic — group 'consumergroupname'

Create Consumer Group for topic:

bash /opt/kafka/bin/kafka-console-consumer.sh — bootstrap-server serverip:9092 — topic newtopic — from-beginning — group consumergroupname — consumer.config /opt/kafka/config/kraft/admin.config

List all ACLs:

bash /opt/kafka/bin/kafka-acls.sh — bootstrap-server serverip:9092 — list — command-config /opt/kafka/config/kraft/admin.config