FABRIC RELEASE NOTES

FABRIC V7.2.2 HOT FIX 8 RELEASE NOTES

These Release Notes describe the new features in Fabric release V7.2.2 HF8 and list bugs that have been fixed since the V7.2.2 HF7 release.

Certification of this Fabric release is based on:

- Cassandra version 4.1.3
- SQLite version 3.44.1.0
- Open JDK Runtime Environment (build 17.0.10+7)
- Confluent Kafka version 7.2.1
- Neo4j 5.12.0 – enterprise
- Elasticsearch – 8.5.3
- AWS OpenSearch – 1.3.4
- PostgreSQL 15.4 (Debian 15.4-1.pgdg120+1)

RESOLVED ISSUES

- iidFinder
    - jvm.iid_finder.options – change default memory allocated to production servers as Min-2, Max-8.
    - Insert iidfinder affinity into a node id template. Add the parameter iidfinder_job:1
    - Support SASL/SCRAM as Kafka authentication.
        - The following configuration should be setup in order to make it work:

      In iifConfig.ini:
        - In kafka section – zookeeper and kafka servers should be configured
            - KAFKA_BOOTSTRAP_SERVERS=<ip>:<port>
            - ZOOKEEPER_BOOTSRTAP_SERVERS=<ip>:<port>
        - In “common_area_kafka_producer”, “delta_kafka_producer” sections - kafka server should be configured
            - BOOTSTRAP_SERVERS=<ip>
        - In “finder_kafka_ssl_properties”, “common_area_kafka_ssl_properties”, and “delta_kafka_ssl_properties” sections the following should be configured:
            - SSL_ENABLED=true
            - SECURITY_PROTOCOL=SASL_SSL
            - TRUSTSTORE_LOCATION=**PATH_TO**/.kafka_ssl/kafka.client.truststore.jks
            - TRUSTSTORE_PASSWORD= truststore password
            - KEYSTORE_LOCATION= **PATH_TO** /.kafka_ssl/kafka.client.keystore.jks
            - KEYSTORE_PASSWORD= keystore password
            - KEY_PASSWORD= keystore password

- SASL_TYPE=SASL_SCRAM
- SASL_USERNAME=SASL user name
- SASL_PASSWORD=SASL password
- SCRAM_HASH_POLICY=SCRAM-SHA-512

In order to use SOR delta the following should be changed in config.ini:

- In “default_pubsub”, “delta_kafka_producer” sections - kafka server should be configured
  - BOOTSTRAP_SERVERS=<ip>:<port>
- In “kafka_ssl_properties”, “delta_kafka_ssl_properties”, and “default_pubsub” sections the following should be configured:
  - SSL_ENABLED=true
  - SECURITY_PROTOCOL=SASL_SSL
  - TRUSTSTORE_LOCATION=**PATH_TO**/.kafka_ssl/kafka.client.truststore.jks
  - TRUSTSTORE_PASSWORD= truststore password
  - KEYSTORE_LOCATION= **PATH_TO** /.kafka_ssl/kafka.client.keystore.jks
  - KEYSTORE_PASSWORD= keystore password
  - KEY_PASSWORD= keystore password
  - SASL_TYPE=SASL_SCRAM
  - SASL_USERNAME=SASL user name
  - SASL_PASSWORD=SASL password
  - SCRAM_HASH_POLICY=SCRAM-SHA-512

- Ticket #38213, resolve older release password encryption failure.