



FABRIC V8.3.2 RELEASE NOTES

- These Release Notes describe the new features in Fabric release V8.3.2 and list bugs that have been fixed since the V8.3.1 release.
- Certification of this Fabric release is based on:
 - Cassandra version 4.1.8
 - SQLite version 3.46.1
 - OpenJDK Runtime Environment 21.0.9+10
 - Confluent Kafka version 8.1.1
 - Neo4j enterprise 5.26.19
 - Elasticsearch 8.5.3 and 7.16.3
 - PostgreSQL 17.5
 - AWS OpenSearch:
 - Cloud: 3.1 and 2.17
 - On prem: 1.3.4

RESOLVED ISSUES

- Ticket #46029 – all results from the inner flow call were loaded into memory when the inner flow actor closed, even if they were not in use. A fix was introduced to prevent loading results into memory on inner flow close.
- Ticket #46899 – the SourceDbQuery actor was enhanced to add double quotes to column names in the SELECT statement only when a column name is special.
- Ticket #46823 – Broadway: Typing the name of an external parameter no longer causes the field to lose focus immediately.
- Ticket #47142 – enhanced Fabric commands to serialize null values and return Double.NaN as null instead of failing.
- Ticket #47104 – Web Studio: the Interface Editor now allows the use of secret managers for the JDBC interface certificate field, with no special pattern required.
- Ticket #47194 – Web Studio – Schema: Show Connected / Successor / Predecessor Nodes is now supported for all node populations.
- During the discovery process, a discrepancy was identified between the PII field count reported by the 'Classification PII Marker' plugin and the actual search graph results filtered by 'pii=true'.
- Ticket #46998 – the discovery process was enhanced to support the Map data type.
- Ticket #47320 – iidFinder – since the Avro format has strict field requirements, the code was updated to verify that the token field is present before accessing it.



FABRIC RELEASE NOTES

- Integrated all fixes from Fabric version 8.3.1 HF3.
- Enhance file name search in the S3 file system interface to properly handle dash characters.
- Resolved 3rd party security vulnerabilities.