## 릴리스 4.0.2312.1

### 알려진 이슈

* 패치 전 센트리 연결을 위해 기존 인증서로 RPC 포트를 열어둔 경우, 패치 후 센트리 자동설치 기능이 동작하지 않을 수 있습니다.

**아래 이슈들은 4.0.2312.2 패키지에서 해결했습니다.**

* SNR#2356 라이선스 미설치 상태에서 노드 이중화 설정을 진행할 수 없는 문제가 있습니다.
* SNR#2359 샘플 앱 호환성 문제가 있습니다.

### 버그 해결

|  |  |
| --- | --- |
| 식별자 | 항목 |
| [SNR#2306](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2306) | case 함수에서 특정 분기 데이터가 없고 모든 출력값이 정수일 때 출력값 타입이 long으로 변환되는 문제 해결 |
| [SNR#2319](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2319) | 앱을 재설치해도 수집 모델 정규화 규칙이 앱 내용으로 업데이트되지 않는 문제 해결 |
| [SNR#2333](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2333) | 멀티 노드 환경에서 분산 쿼리 실행 시 쿼리 결과 파일이 삭제되지 않는 문제 해결 |
| [SNR#2339](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2339) | CTI IP 피드와 도메인 피드 수신이 실패하는 문제 해결 |
| [SNR#2341](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2341) | 4.0.2312.0 패키지 신규 설치 시 분석 서버 노드 B에서 event 테이블 인덱스가 생성되지 않는 문제 해결 |
| [SNR#2342](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2342) | 리눅스 환경에 센트리 자동 설치 후 서버 재기동 시 센트리가 무한 재부팅되는 문제 해결 |
| [SNR#2343](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2343) | 4.0.2312.0 버전에서 Sonar Light의 SQLite 모드로 설치 시 오류가 발생하는 문제 해결 |

### 상세 내역

#### SNR#2306 case 함수에서 특정 분기 데이터가 없고 모든 출력값이 정수일 때 출력값 타입이 long으로 변환되는 문제 해결

로그프레소 쿼리문에서 case() 함수 사용 시, 특정 분기에 속하는 데이터가 한 건도 없고, case 함수 출력값이 정수(int) 타입이고, 입력 데이터가 columnar 형태일 때, case() 함수 출력 타입이 정수(int)가 아닌 long 유형으로 출력되는 문제가 해결되었습니다.

| eval test\_field=case(true,1,false,2,0)| eval type\_of\_test\_field=typeof(test\_field) | # 패치 전: int가 아닌 long 출력. 패치 후: int 출력

#### SNR#2319 앱을 재설치해도 수집 모델 정규화 규칙이 앱 내용으로 업데이트되지 않는 문제 해결

로그프레소 앱을 재설치하거나 업데이트할 때 수집 모델 정규화 규칙의 스트림 쿼리가 앱의 내장된 내용으로 업데이트되지 않는 문제가 해결되었습니다. 패치 후 앱 재설치 시 사용자가 수정한 수집 모델 정규화 규칙의 스트림 쿼리는 앱 내장 스트림 쿼리로 초기화됩니다.

#### SNR#2333 멀티 노드 환경에서 분산 쿼리 실행 시 쿼리 결과 파일이 삭제되지 않는 문제 해결

멀티 노드 환경에서 분산 쿼리 실행 시 쿼리 결과 파일이 삭제되지 않고 남아있는 문제를 해결했습니다. 패치 전, 해당 이슈로 인해 쿼리 결과 파일이 너무 많이 생기고 디스크가 고갈되면서 로그프레소가 정상 운영되지 않는 문제가 있었습니다.

#### SNR#2339 CTI IP 피드와 도메인 피드 수신이 실패하는 문제 해결

로그프레소 CTI 피드 중 IP 피드와 도메인 피드 원천 데이터의 source\_id 값이 null인 경우가 존재하여 아래와 같이 NPE 에러가 발생하며 수신에 실패하는 문제를 해결했습니다.

[2024-01-11 15:48:33.104] ERROR (LogpressoCtiConnector) - sonar cti client: request feed failed - null[2024-01-11 15:48:33.104] WARN (ScriptRunner) - script runner:java.lang.reflect.InvocationTargetException at java.base/jdk.internal.reflect.NativeMethodAccessorImpl.invoke0(Native Method) at java.base/jdk.internal.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:62) at java.base/jdk.internal.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43) at java.base/java.lang.reflect.Method.invoke(Method.java:566) at org.araqne.console.ScriptRunner.invokeScript(ScriptRunner.java:224) at org.araqne.console.ScriptRunner.run(ScriptRunner.java:205) at java.base/java.lang.Thread.run(Thread.java:829)Caused by: java.lang.IllegalStateException: java.lang.NullPointerException at com.logpresso.sonar.cti.impl.LogpressoCtiConnector.getThreatFeeds(LogpressoCtiConnector.java:52) at com.logpresso.sonar.cti.impl.LogpressoCtiFeedSyncer.\_\_M\_retrieveFeeds(LogpressoCtiFeedSyncer.java:145) at com.logpresso.sonar.cti.impl.LogpressoCtiFeedSyncer.retrieveFeeds(LogpressoCtiFeedSyncer.java) at com.logpresso.sonar.cti.impl.LogpressoCtiFeedSyncer.\_\_M\_sync(LogpressoCtiFeedSyncer.java:123) at com.logpresso.sonar.cti.impl.LogpressoCtiFeedSyncer.sync(LogpressoCtiFeedSyncer.java) at com.logpresso.sonar.script.ThreatFeedScript.syncThreatFeed(ThreatFeedScript.java:49) ... 7 moreCaused by: java.lang.NullPointerException at com.logpresso.sonar.cti.LogpressoCtiFeed.parse(LogpressoCtiFeed.java:125) at com.logpresso.sonar.cti.impl.LogpressoCtiConnector.parse(LogpressoCtiConnector.java:61) at com.logpresso.sonar.cti.impl.LogpressoCtiConnector.getThreatFeeds(LogpressoCtiConnector.java:49) ... 12 more

#### SNR#2341 4.0.2312.0 패키지 신규 설치 시 분석 서버 노드 B에서 event 테이블 인덱스가 생성되지 않는 문제 해결

4.0.2312.0 버전에 포함된 [SNR#1980](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1980) 이슈에서 로그프레소 소나 설치 시 이벤트 관련 테이블에 인덱스가 자동으로 생성되는 기능이 추가되었으나, 분석 서버 노드 A에만 인덱스가 생성되고 노드 B에서는 이벤트 테이블에 인덱스 생성되지 않는 문제가 있어 이를 해결했습니다.

#### SNR#2342 리눅스 환경에 센트리 자동 설치 후 서버 재기동 시 센트리가 무한 재부팅되는 문제 해결

센트리 자동 설치 기능으로 리눅스 서버에 센트리 설치 후 리눅스 서버가 재기동될 경우 센트리가 정상적으로 부팅되지 않고 계속 재부팅되는 문제가 해결되었습니다.

#### SNR#2343 4.0.2312.0 버전에서 Sonar Light의 SQLite 모드로 설치 시 오류가 발생하는 문제 해결

4.0.2312.0 버전에서 Sonar Light가 SQLite 모드로 설치 시 아래와 같이 SQL 오류가 발생하는 문제를 해결했습니다.

[2024-01-15 10:37:15,868] ERROR (MessageBusImpl) - araqne msgbus: message handler failedjava.lang.IllegalStateException: cannot create logger model: e1d84de7-4bc4-4cd0-87c9-a782e70eb202 at com.logpresso.sonar.api.impl.LoggerServiceImpl.\_\_M\_createLoggerModel(LoggerServiceImpl.java:376) at com.logpresso.sonar.api.impl.LoggerServiceImpl.createLoggerModel(LoggerServiceImpl.java) at com.logpresso.sonar.msgbus.LoggerPlugin.\_\_M\_createLoggerModel(LoggerPlugin.java:484) at com.logpresso.sonar.msgbus.LoggerPlugin.createLoggerModel(LoggerPlugin.java)Caused by: java.lang.IllegalStateException: sonar sql [INSERT INTO sonar\_extractor\_models (guid, name, logger\_model\_id, table\_schema\_id, parser\_id, filter, stream\_query, stream\_interval) VALUES (?,?,?,?,?,?,?,?)] failure at com.logpresso.sonar.dom.impl.SqlConnectorImpl.\_\_M\_execute(SqlConnectorImpl.java:275) at com.logpresso.sonar.dom.impl.SqlConnectorImpl.execute(SqlConnectorImpl.java) at com.logpresso.sonar.api.impl.LoggerServiceImpl.\_\_M\_createExtractorModel(LoggerServiceImpl.java:514) at com.logpresso.sonar.api.impl.LoggerServiceImpl.createExtractorModel(LoggerServiceImpl.java) at com.logpresso.sonar.api.impl.LoggerServiceImpl.\_\_M\_createExtractors(LoggerServiceImpl.java:475) at com.logpresso.sonar.api.impl.LoggerServiceImpl.createExtractors(LoggerServiceImpl.java) at com.logpresso.sonar.api.impl.LoggerServiceImpl.\_\_M\_createLoggerModel(LoggerServiceImpl.java:369) at com.logpresso.sonar.api.impl.LoggerServiceImpl.createLoggerModel(LoggerServiceImpl.java) at com.logpresso.sonar.msgbus.LoggerPlugin.\_\_M\_createLoggerModel(LoggerPlugin.java:484) at com.logpresso.sonar.msgbus.LoggerPlugin.createLoggerModel(LoggerPlugin.java) at java.base/jdk.internal.reflect.NativeMethodAccessorImpl.invoke0(Native Method) at java.base/jdk.internal.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:62) at java.base/jdk.internal.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43) at java.base/java.lang.reflect.Method.invoke(Method.java:566) at org.araqne.msgbus.handler.MsgbusPluginHandler.\_\_M\_handleMessage(MsgbusPluginHandler.java:197) at org.araqne.msgbus.handler.MsgbusPluginHandler.handleMessage(MsgbusPluginHandler.java) at org.araqne.msgbus.impl.MessageBusImpl$TaskRunner.\_\_M\_invokeMessageHandler(MessageBusImpl.java:591) at org.araqne.msgbus.impl.MessageBusImpl$TaskRunner.invokeMessageHandler(MessageBusImpl.java) at org.araqne.msgbus.impl.MessageBusImpl$TaskRunner.\_\_M\_run(MessageBusImpl.java:580) at org.araqne.msgbus.impl.MessageBusImpl$TaskRunner.run(MessageBusImpl.java) at java.base/java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1128) at java.base/java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:628) at java.base/java.lang.Thread.run(Thread.java:834)Caused by: org.sqlite.SQLiteException: [SQLITE\_CONSTRAINT\_NOTNULL] A NOT NULL constraint failed (NOT NULL constraint failed: sonar\_extractor\_models.table\_schema\_id) at org.sqlite.core.DB.newSQLException(DB.java:1179) at org.sqlite.core.DB.newSQLException(DB.java:1190) at org.sqlite.core.DB.execute(DB.java:985) at org.sqlite.jdbc3.JDBC3PreparedStatement.lambda$execute$0(JDBC3PreparedStatement.java:57) at org.sqlite.jdbc3.JDBC3Statement.withConnectionTimeout(JDBC3Statement.java:454) at org.sqlite.jdbc3.JDBC3PreparedStatement.execute(JDBC3PreparedStatement.java:52) at org.logpresso.jdbc.JdbcPoolPreparedStatement.execute(JdbcPoolPreparedStatement.java:176) at com.logpresso.sonar.dom.impl.SqlConnectorImpl.\_\_M\_execute(SqlConnectorImpl.java:260) ... 22 more