## 릴리스 4.0.2303.0

### 기능 개선

|  |  |
| --- | --- |
| 식별자 | 항목 |
| [ENT#4019](https://docs.logpresso.com/ko/enterprise/4.0/issues/ENT4019) | 로그프레소 시스로그 서버 및 클라이언트의 상태를 확인할 수 있는 쿼리 커맨드 추가 |
| [ENT#4269](https://docs.logpresso.com/ko/enterprise/4.0/issues/ENT4269) | 윈도우 이벤트로그 수집기에 윈도우 이벤트 ID 제외 옵션 추가 |
| [ENT#4274](https://docs.logpresso.com/ko/enterprise/4.0/issues/ENT4274) | CEF 파서 출력 필드 정규화 |
| [ENT#4345](https://docs.logpresso.com/ko/enterprise/4.0/issues/ENT4345) | 접속 프로파일 메뉴에 멀티라인 입력창 지원 기능 추가 |

### 버그 해결

|  |  |
| --- | --- |
| 식별자 | 항목 |
| [ENT#3897](https://docs.logpresso.com/ko/enterprise/4.0/issues/ENT3897) | order와 join 커맨드의 에러 코드 중복 해결 |
| [ENT#4021](https://docs.logpresso.com/ko/enterprise/4.0/issues/ENT4021) | limit 커맨드가 포함된 분산 쿼리 실행 시 낮은 확률로 쿼리 데드락이 발생하는 문제 해결 |
| [ENT#4282](https://docs.logpresso.com/ko/enterprise/4.0/issues/ENT4282) | 대시보드 탭 좌우 스크롤 버튼 추가 |
| [ENT#4391](https://docs.logpresso.com/ko/enterprise/4.0/issues/ENT4391) | UDP 시스로그 수신 시 버퍼 초과 패킷을 파일로 저장할 때 유실이 발생하는 문제 해결 |
| [ENT#4392](https://docs.logpresso.com/ko/enterprise/4.0/issues/ENT4392) | 웹콘솔에서 파서 설정 변경 후 CLI 에서 logapi.parsers 명령어를 수행하면 NPE 에러가 발생하는 문제 해결 |
| [ENT#4393](https://docs.logpresso.com/ko/enterprise/4.0/issues/ENT4393) | 멤버 권한 계정이 계정 메뉴로 진입하면 에러 로그가 발생하는 문제 해결 |
| [ENT#4409](https://docs.logpresso.com/ko/enterprise/4.0/issues/ENT4409) | 쿼리문에 긴 문자열이 포함된 경우 쿼리 실행 현황이 겹쳐보이는 문제 해결 |
| [ENT#4423](https://docs.logpresso.com/ko/enterprise/4.0/issues/ENT4423) | 패키지 관리 화면에서 상태 열 버튼과 아이콘이 어긋나게 표시되는 문제 해결 |
| [ENT#4430](https://docs.logpresso.com/ko/enterprise/4.0/issues/ENT4430) | 외부 프로그램 수집기, 윈도우 네트워크 대역폭 사용률 수집기, 윈도우 성능카운터 수집기에서 윈도우 API 호출 오류 시 메모리 누수 발생 해결 |
| [ENT#4440](https://docs.logpresso.com/ko/enterprise/4.0/issues/ENT4440) | 센트리 수집기에 호스트 태그 설정을 입력하지 않은 경우 센트리의 GUID를 호스트 태그로 수집하도록 수정 |
| [ENT#4442](https://docs.logpresso.com/ko/enterprise/4.0/issues/ENT4442) | sendsyslog 쿼리 커맨드의 src 옵션 사용시, 네이티브 메모리 할당에 실패할 경우 로그프레소 서버가 강제 종료되는 문제 해결 |
| [ENT#4463](https://docs.logpresso.com/ko/enterprise/4.0/issues/ENT4463) | pivot, timechart 등 집계 쿼리 커맨드 사용 시 컬럼 개수 제한 기능 추가 |
| [SNR#2058](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2058) | table 쿼리 커맨드로 특정 노드에 대해 와일드카드 조회 시 NPE 에러가 발생하며 쿼리가 실패하는 문제 해결 |

### 상세 내역

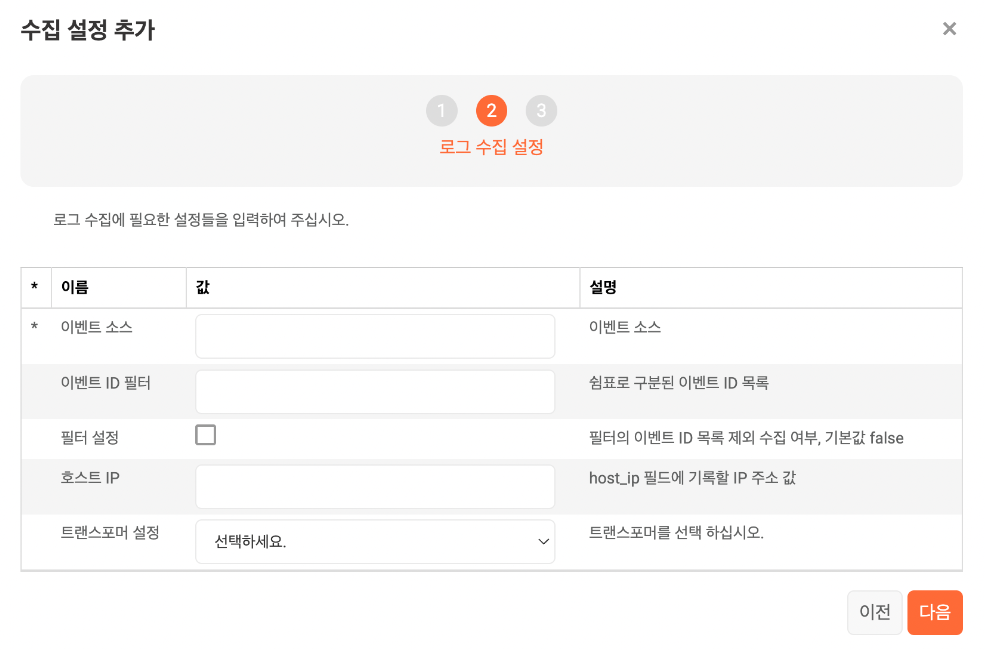
#### ENT#4019 로그프레소 시스로그 서버 및 클라이언트의 상태를 확인할 수 있는 쿼리 커맨드 추가

로그프레소 시스로그 서버와 클라이언트의 상태를 조회할 수 있는 쿼리 커맨드들이 추가되었습니다.

* 로그프레소 시스로그 서버 상태 조회
* 외부 서버(시스로그 클라이언트)에서 전송하는 시스로그를 수신하는 로그프레소 시스로그 서버의 상태를 확인합니다.
* 문법
* system-syslog-servers
* 출력 필드
* profile: 시스로그 서버의 이름
* listen\_ip: 시스로그 서버의 수신 IP주소
* listen\_port: 시스로그 서버의 포트 번호
* protocol: 시스로그 서버가 수신하는 프로토콜 (TCP/UDP)
* charset: 수신하는 시스로그의 문자열 인코딩
* rcvd\_pkts: 수신한 패킷 수
* drop\_pkts: 드랍된 패킷 수
* last\_syscall: 마지막으로 시스로그 서버의 상태를 확인한 시각
* 로그프레소 시스로그 클라이언트 상태 조회
* 로그프레소 시스로그 서버로 시스로그를 전송해주는 클라이언트의 상태를 확인합니다.
* 문법
* system-syslog-clients
* 출력 필드
* profile: 시스로그 서버의 이름
* client\_ip: 시스로그 클라이언트의 IP 주소
* listen\_ip: 시스로그 서버의 수신 IP주소
* listen\_port: 시스로그 서버의 포트 번호
* protocol: 시스로그 서버가 수신하는 프로토콜 (TCP/UDP)
* count: 시스로그 수집 건수
* first\_seen: 시스로그를 처음 수신한 시각
* last\_seen: 시스로그를 마지막으로 수신한 시각

#### ENT#4269 윈도우 이벤트로그 수집기에 윈도우 이벤트 ID 제외 옵션 추가

윈도우 이벤트로그 수집기에 '필터 설정' 옵션이 추가되었습니다. '필터 설정' 옵션을 활성화하지 않으면 기존처럼 '이벤트 ID 필터'에 입력된 이벤트 ID와 매칭하는 이벤트로그를 수집합니다. '필터 설정' 옵션을 활성화하면 '이벤트 ID 필터'에 입력된 이벤트 ID와 매칭하지 않는 이벤트로그를 수집합니다.



#### ENT#4274 CEF 파서 출력 필드 정규화

CEF 파서의 출력 필드에 대해 정규화된 필드 이름과 타입을 적용하였습니다. 파서 생성시 버전을 2로 설정하면 파싱 결과가 정규화된 필드로 출력됩니다. 버전을 설정하지 않고 생성하거나 기존 배포 버전에서 생성한 파서는 정규화가 적용되지 않은 필드가 출력됩니다.



변경되는 필드들은 다음과 같습니다.

|  |  |  |
| --- | --- | --- |
| 변경전 | 변경후 | 타입 |
| src | src\_ip | IP |
| spt | src\_port | INT |
| dst | dst\_ip | IP |
| dpt | dst\_port | INT |
| sourceTranslatedAddress | nat\_src\_ip | IP |
| sourceTranslatedPort | nat\_src\_port | INT |
| destinationTranslatedAddress | nat\_dst\_ip | IP |
| destinationTranslatedPort | nat\_dst\_port | INT |
| dvc | device\_ip | IP |
| dvchost | device\_host | STRING |
| dvcmac | device\_mac | STRING |
| dvcpid | device\_pid | LONG |
| sourceDnsDomain | src\_domain | STRING |
| sourceServiceName | src\_service | STRING |
| destinationDnsDomain | dst\_domain | STRING |
| destinationServiceName | dst\_service | STRING |
| shost | src\_host | STRING |
| smac | src\_mac | STRING |
| dhost | dst\_host | STRING |
| dmac | dst\_mac | STRING |
| suid | src\_user\_id | STRING |
| suser | src\_user | STRING |
| duid | dst\_user\_id | STRING |
| duser | dst\_user | STRING |
| spid | src\_pid | LONG |
| sproc | src\_process | STRING |
| dpid | dst\_pid | LONG |
| dproc | dst\_process | STRING |
| fileCreateTime | file\_ctime | DATE |
| fileModificationTime | file\_mtime | DATE |
| fname | file\_name | STRING |
| filePath | file\_path | STRING |
| fileType | file\_type | STRING |
| fsize | file\_size | LONG |
| fileHash | file\_hash | STRING |
| in | rcvd\_bytes | LONG |
| out | sent\_bytes | LONG |
| proto | protocol | STRING |
| app | app | STRING |
| act | action | STRING |
| cat | category | STRING |
| cnt | event\_count | INT |

#### ENT#4345 접속 프로파일 메뉴에 멀티라인 입력창 지원 기능 추가

접속 프로파일 메뉴에 멀티라인 입력창 지원 기능이 추가되었습니다. 멀티라인 입력이 필요한 경우 멀티라인 입력창을 이용할 수 있습니다.

#### ENT#3897 order와 join 커맨드의 에러 코드 중복 해결

order와 join 쿼리 커맨드가 중복된 에러 코드를 사용하여 order 쿼리 커맨드 에러가 발생했을 때 join 쿼리 커맨드의 에러 메시지가 표시되는 문제가 해결되었습니다.

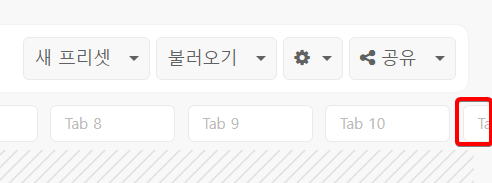
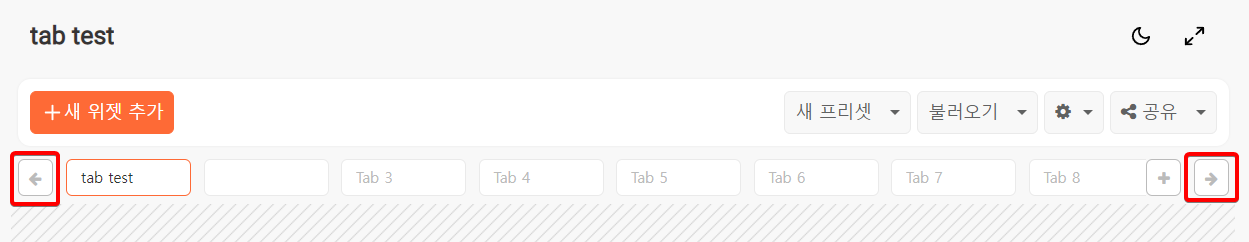
#### ENT#4021 limit 커맨드가 포함된 분산 쿼리 실행 시 낮은 확률로 쿼리 데드락이 발생하는 문제 해결

분산 쿼리 수행 시 쿼리문에 limit 커맨드가 포함된 경우, 쿼리 종료 과정에서 낮은 확률로 데드락이 발생하는 문제가 있었습니다. 쿼리 데드락이 발생하면 쿼리 수행에 할당된 리소스가 해제되지 않았고, 이 현상이 누적되면 점점 할당 가능한 리소스가 줄어들어 웹UI에 접속이 되지 않는 상황까지도 발생했습니다.패치 버전에서는 limit 커맨드 수행 과정을 분산 쿼리 수행에 좀 더 적합하도록 thread-safe 하게 변경하여 데드락이 발생할 여지를 줄이는 방법으로 해당 문제를 해결했습니다.

#### ENT#4282 대시보드 탭 좌우 스크롤 버튼 추가

기존 배포 버전에서는 대시보드 화면에서 탭을 많이 생성할 경우 나중에 생성된 탭이 화면 밖으로 벗어나서 탭이 제대로 표시되지 않거나 선택할 수 없는 문제가 있었습니다.

패치 후에는 대시보드 탭 항목을 좌우로 이동할 수 있는 스크롤 버튼이 추가되었습니다. 탭 좌우 스크롤 버튼을 사용하여 모든 대시보드 탭을 조회할 수 있습니다.

* 패치 전 - 대시보드 탭이 화면 밖으로 벗어나서 제대로 표시되지 않음
* 패치 후 - 이전/다음 탭 이동 버튼이 추가되어 탭 선택 가능

#### ENT#4391 UDP 시스로그 수신 시 버퍼 초과 패킷을 파일로 저장할 때 유실이 발생하는 문제 해결

해당 이슈는 로그프레소 4.0.2205.0 이상, 4.0.2212.0 이하 버전에서 발생합니다.

시스로그 서버에서 UDP 포트로 시스로그를 수신하다 버퍼 용량이 가득 차게 되어 초과 수신 패킷을 파일에 저장할 때, 패킷 내용의 일부가 유실되는 문제를 해결했습니다.

#### ENT#4392 웹콘솔에서 파서 설정 변경 후 CLI 에서 logapi.parsers 명령어를 수행하면 NPE 에러가 발생하는 문제 해결

파서 메뉴에서 파서의 설정을 변경한 다음 CLI 에서 logapi.parsers 명령어를 수행하면 파서 목록이 표시되지 않고 아래와 같은 NPE(NullPointerException) 에러가 발생하는 문제가 해결되었습니다.

* CLI 명령 수행 결과

logpresso> logapi.parsers Log Parser Profiles --------------------- name=firepower2, factory=firepower, configs={ver=2} java.lang.NullPointerException

* 에러 로그

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:834) Caused by: java.lang.NullPointerException at org.araqne.log.api.LogParserProfile.toString(LogParserProfile.java:71) at org.araqne.script.ScriptContextImpl.println(ScriptContextImpl.java:175) at org.araqne.log.api.impl.LogApiScript.parsers(LogApiScript.java:123) ... 7 more

#### ENT#4393 멤버 권한 계정이 계정 메뉴로 진입하면 에러 로그가 발생하는 문제 해결

해당 이슈는 로그프레소 4.0.2205.0 이상, 4.0.2212.0 이하 버전에서 발생합니다.

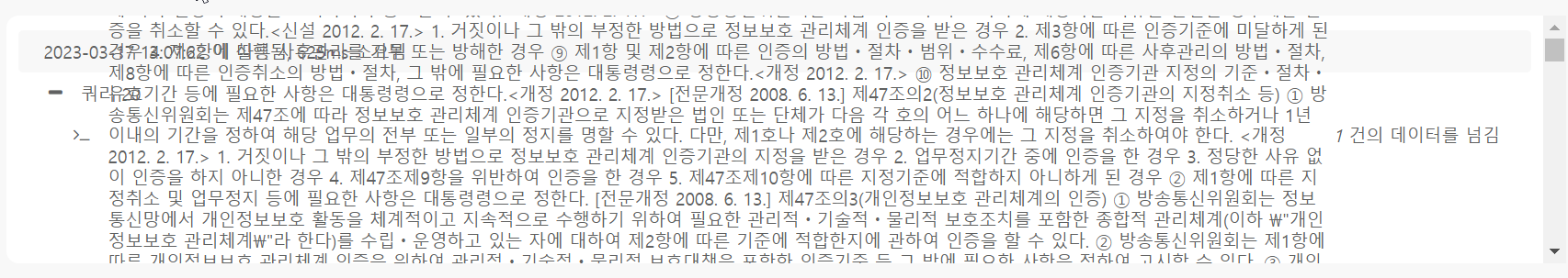
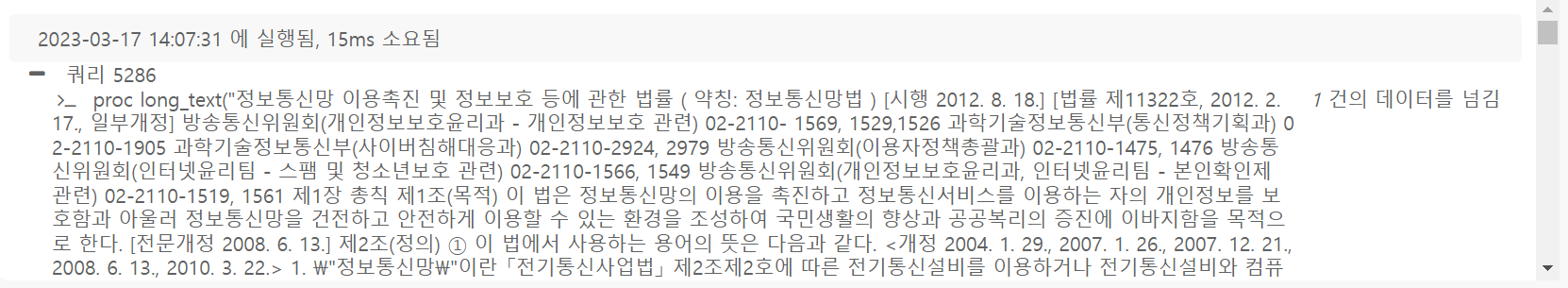
멤버 권한 계정으로 계정 메뉴 진입 시, 계정 정보는 정상적으로 표시되며 동작에는 문제가 없지만 araqne.log 파일에 에러 로그가 발생하던 문제가 해결되었습니다. 기존 배포 버전에서 발생하던 에러 로그는 다음과 같습니다.

[2022-10-18 18:02:55,530] WARN (MessageBusImpl) - araqne msgbus: security violation [domain=localhost, admin\_login\_name=test\_member\_error, method=com.logpresso.core.msgbus.UserPlugin.getUsers] from remote [xxx.xxx.xxx.xxx][2022-10-18 18:02:55,530] ERROR (MessageBusImpl) - araqne msgbus: message handler failedjava.lang.SecurityException: you are not allowed to list users. at com.logpresso.core.msgbus.UserPlugin.\_\_M\_getUsers(UserPlugin.java:239)

#### ENT#4409 쿼리문에 긴 문자열이 포함된 경우 쿼리 실행 현황이 겹쳐보이는 문제 해결

해당 이슈는 로그프레소 4.0.2205.0 이상, 4.0.2212.0 이하 버전에서 발생합니다.

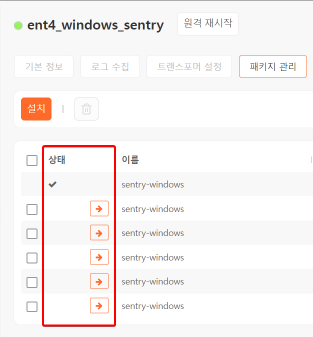
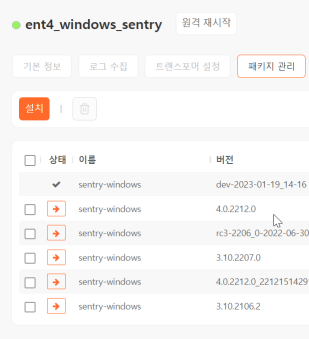
쿼리문에 긴 문자열이 포함된 경우 쿼리 실행 현황이 겹쳐보이는 문제가 해결되었습니다.

* 패치 전: 쿼리문이 서로 겹치는 문제 발생
* 패치 후: 쿼리문이 겹치지 않고 정상적으로 표시

#### ENT#4423 패키지 관리 화면에서 상태 열 버튼과 아이콘이 어긋나게 표시되는 문제 해결

해당 이슈는 로그프레소 4.0.2205.0 이상, 4.0.2212.0 이하 버전에서 발생합니다.

시스템 관리 > 패키지 관리 화면과 수집 설정 > 센트리 > 패키지 관리 화면에서 '상태' 열의 버튼 위치가 어긋나고, 열 너비가 너무 넓게 표시되는 문제가 해결되었습니다.

* 패치 전: 패키지 전환 버튼 위치가 어긋나있고 상태 열 너비가 너무 넓음
* 패치 후: 패키지 전환 버튼 위치와 상태 열 너비가 자연스럽게 표시됨

#### ENT#4430 외부 프로그램 수집기, 윈도우 네트워크 대역폭 사용률 수집기, 윈도우 성능카운터 수집기에서 윈도우 API 호출 오류 시 메모리 누수 발생 해결

로그프레소 ENT 서버의 외부 프로그램 수집기, 윈도우 센트리의 윈도우 네트워크 대역폭 사용률 수집기, 윈도우 성능카운터 수집기에서 윈도우 API를 호출할 때 오류가 발생하면 메모리가 누수되는 현상을 해결했습니다.

#### ENT#4440 센트리 수집기에 호스트 태그 설정을 입력하지 않은 경우 센트리의 GUID를 호스트 태그로 수집하도록 수정

센트리의 모든 수집기에 대해 호스트 태그를 설정하지 않을 시 \_host 필드에 센트리의 GUID 값을 할당하도록 변경했습니다.

#### ENT#4442 sendsyslog 쿼리 커맨드의 src 옵션 사용시, 네이티브 메모리 할당에 실패할 경우 로그프레소 서버가 강제 종료되는 문제 해결

sendsyslog 쿼리 커맨드에 src 옵션을 지정하여 수행하다 네이티브 메모리 할당에 실패하더라도 로그프레소 서버가 강제 종료되지 않도록 오류 처리를 개선하였습니다.

#### ENT#4463 pivot, timechart 등 집계 쿼리 커맨드 사용 시 컬럼 개수 제한 기능 추가

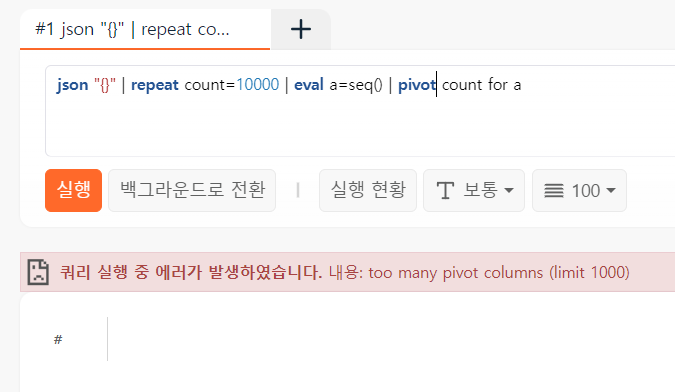
pivot이나 timechart 등 집계 쿼리 커맨드 사용 시 결과 컬럼이 너무 많이 생겨 OOM(OutOfMemory) 에러가 발생하는 것을 방지하기 위해 생성 컬럼 개수를 제한하는 기능을 추가했습니다. 컬럼 개수 제한은 기본값으로 1000개이며, araqne.logdb.column\_generation\_limit 옵션을 사용해 부팅 스크립트나 CLI 커맨드로 변경 가능합니다. 집계 쿼리 커맨드 결과 컬럼 개수가 컬럼 개수 제한을 초과하는 경우 에러 메시지와 함께 쿼리 실행이 중단됩니다.

* 부팅 옵션 문법

-Daraqne.logdb.column\_generation\_limit=1000

* CLI에서 적용 방법

set araqne.logdb.column\_generation\_limit=1000

* 컬럼 개수 제한 도달 시 에러 메시지

#### SNR#2058 table 쿼리 커맨드로 특정 노드에 대해 와일드카드 조회 시 NPE 에러가 발생하며 쿼리가 실패하는 문제 해결

table 커맨드로 단일 노드에 대해 와일드카드 조회 시, NPE(NullPointerException) 에러가 발생하며 쿼리가 실패하는 문제가 해결되었습니다. 문제가 발생했던 쿼리의 형태는 다음과 같습니다.

table n2:t\*

발생했던 에러 로그는 다음과 같습니다.

[2023-03-06 22:48:14,722] ERROR (LogQueryPlugin) - araqne logdb: cannot create queryjava.lang.NullPointerException at com.logpresso.query.planner.DistributedQueryPlanner.\_\_M\_expandToAsteriskRemoteStorageObjectSpec(DistributedQueryPlanner.java:1085) at com.logpresso.query.planner.DistributedQueryPlanner.expandToAsteriskRemoteStorageObjectSpec(DistributedQueryPlanner.java) at com.logpresso.query.planner.DistributedQueryPlanner.\_\_M\_expandToRemoteStorageObjectSpec(DistributedQueryPlanner.java:1290) at com.logpresso.query.planner.DistributedQueryPlanner.expandToRemoteStorageObjectSpec(DistributedQueryPlanner.java) at com.logpresso.query.planner.DistributedQueryPlanner.\_\_M\_expandToRemoteStorageObjectSpecs(DistributedQueryPlanner.java:1052) at com.logpresso.query.planner.DistributedQueryPlanner.expandToRemoteStorageObjectSpecs(DistributedQueryPlanner.java) at com.logpresso.query.planner.DistributedQueryPlanner.\_\_M\_expandStorageObjectSpecs(DistributedQueryPlanner.java:1038) at com.logpresso.query.planner.DistributedQueryPlanner.expandStorageObjectSpecs(DistributedQueryPlanner.java) at com.logpresso.query.planner.DistributedQueryPlanner.\_\_M\_classifySources(DistributedQueryPlanner.java:999) at com.logpresso.query.planner.DistributedQueryPlanner.classifySources(DistributedQueryPlanner.java) at com.logpresso.query.planner.DistributedQueryPlanner.\_\_M\_planRecursively(DistributedQueryPlanner.java:264) at com.logpresso.query.planner.DistributedQueryPlanner.planRecursively(DistributedQueryPlanner.java) at com.logpresso.query.planner.DistributedQueryPlanner.\_\_M\_plan(DistributedQueryPlanner.java:244) at com.logpresso.query.planner.DistributedQueryPlanner.plan(DistributedQueryPlanner.java) at org.araqne.logdb.query.engine.QueryServiceImpl.\_\_M\_createQuery(QueryServiceImpl.java:374) at org.araqne.logdb.query.engine.QueryServiceImpl.createQuery(QueryServiceImpl.java) at org.araqne.logdb.msgbus.LogQueryPlugin.\_\_M\_createQuery(LogQueryPlugin.java:343) at org.araqne.logdb.msgbus.LogQueryPlugin.createQuery(LogQueryPlugin.java) at jdk.internal.reflect.GeneratedMethodAccessor36.invoke(Unknown Source) 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:201) at org.araqne.msgbus.handler.MsgbusPluginHandler.handleMessage(MsgbusPluginHandler.java) at org.araqne.msgbus.impl.MessageBusImpl$TaskRunner.\_\_M\_invokeMessageHandler(MessageBusImpl.java:579) at org.araqne.msgbus.impl.MessageBusImpl$TaskRunner.invokeMessageHandler(MessageBusImpl.java) at org.araqne.msgbus.impl.MessageBusImpl$TaskRunner.\_\_M\_run(MessageBusImpl.java:569) at org.araqne.msgbus.impl.MessageBusImpl$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:829)