## 릴리스 4.0.2312.0

### 알려진 이슈

* 패치 전 센트리 연결을 위해 기존 인증서로 RPC 포트를 열어둔 경우, 패치 후 센트리 자동설치 기능이 동작하지 않을 수 있습니다.
* 신규 설치 시 ENT UI 기본 포트가 8888에서 8443으로 변경되었습니다.

**아래 이슈들은 4.0.2312.2 패키지에서 해결했습니다.**

* SNR2356 라이선스 미설치 상태에서 노드 이중화 설정을 진행할 수 없는 문제가 있습니다.
* SNR2359 샘플 앱 호환성 문제가 있습니다.

**아래 이슈들은 4.0.2312.1 패키지에서 해결했습니다.**

* SNR2319 앱을 재설치해도 수집 모델 정규화 규칙이 앱 내용으로 업데이트되지 않는 문제가 있습니다.
* SNR2306 case 쿼리문에서 특정 분기에 속하는 데이터가 없고 모든 출력값이 정수(int) 유형일 때 출력값 타입이 long으로 변환되는 문제가 있습니다.
* SNR2333 멀티 노드 환경에서 분산 쿼리 실행 시 쿼리 결과 파일이 삭제되지 않는 문제가 있습니다.
* SNR2339 CTI IP 피드와 도메인 피드 수신이 실패하는 문제가 있습니다.
* SNR2341 4.0.2312.0 버전을 멀티 노드 구성으로 신규 설치할 경우 분석 서버 노드 B에서 event 테이블 인덱스가 생성되지 않는 문제가 있습니다.
* SNR2342 리눅스 환경에 센트리 자동 설치 후 서버 재기동 시 센트리가 무한 재부팅되는 문제가 있습니다.
* SNR2343 4.0.2312.0 버전에서 Sonar Light의 SQLite 모드로 설치 시 오류가 발생하는 문제가 있습니다.

### 업그레이드 주의사항

* SNR2227 내장 JDBC 드라이버 플러그인 전환으로 인해 기존에 내장되어 있던 JDBC 드라이버가 패키지에서 제거되었습니다. MariaDB, MySQL, SQLite, Oracle 이외의 JDBC 드라이버는 로그프레소 스토어에서 앱을 다운로드하여 설치하시길 바랍니다.
* araqne-core 버전이 4.0.0으로 업데이트 되었습니다.
* 센트리 자동 설치 기능으로 설치된 로그프레소 센트리는 로그프레소 런처를 통해 araqne-core를 실행합니다.
* 인증서 발급 관리 기능이 추가되면서 인증서가 각각 sonar-ca -> logpresso-ca, sonar-base -> logpresso-base, sonar-web -> logpresso-web 으로 변경되었습니다. 업그레이드 시 인증서 변경을 반영하여 RPC 포트 및 웹 서버 포트를 다시 열어야 합니다.
* 서버 인증서 설정을 변경하지 않으면 센트리 자동 설치 시 RPC 접속에 실패합니다.
* import 쿼리 명령어에서 create 옵션이 제거되었습니다.

### 메인 피쳐

|  |  |
| --- | --- |
| 식별자 | 항목 |
| [SNR#2138](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2138) | 앱 관리 기능 추가 |
| [SNR#2046](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2046) | CTI 침해지표 피드 추가 |
| [SNR#1503](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1503) | 센트리 자동 설치 및 인증서 관리 기능 추가 |
| [SNR#1812](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1812) | 룩업 기능 추가 |
| [SNR#2065](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2065) | 예약된 쿼리 기능 추가 |

### 신규 기능

|  |  |
| --- | --- |
| 식별자 | 항목 |
| [SNR#2144](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2144) | 트리맵 차트 위젯 유형 추가 |
| [SNR#2222](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2222) | 테이블 보관 주기 수정 기능 추가 |
| [SNR#2264](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2264) | lastindexof 함수 추가 |

### 기능 개선

|  |  |
| --- | --- |
| 식별자 | 항목 |
| [SNR#1498](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1498) | 동일 계정 동시 접속 방지 기능 추가 |
| [SNR#2148](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2148) | 위젯 종속 변수 최소값 및 최대값 옵션 추가 |
| [SNR#2173](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2173) | SFTP 멀티 로테이션 수집기 하위 디렉토리 순회 기능 추가 |
| [SNR#2174](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2174) | 디렉토리 와처 수집기에 삭제된 파일의 수집 상태를 파기하는 옵션 추가 |
| [SNR#2177](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2177) | matchnet 쿼리 명령어에 매칭 결과 필드를 반환하는 tag 옵션 추가 |
| [SNR#2227](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2227) | JDBC 드라이버 플러그인 지원 |
| [SNR#2237](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2237) | 사용자 정의 필터 변경 사항이 확률적으로 동기화되지 않는 문제 해결 |
| [SNR#2267](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2267) | sonar-add-address-batch 쿼리 명령어에 period 옵션 추가 |
| [SNR#2274](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2274) | 대시보드 조회 시 불필요한 감사 로그 기록 제거 |
| [SNR#2275](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2275) | iplookup 쿼리 명령어 성능 개선, company 옵션 필수 여부를 선택으로 변경 |
| [SNR#2278](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2278) | import 쿼리 명령어에서 create 옵션 제거 |

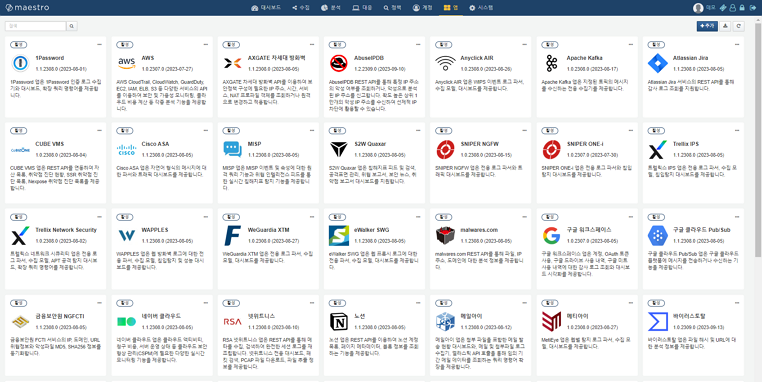
### 버그 해결

|  |  |
| --- | --- |
| 식별자 | 항목 |
| [SNR#1240](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1240) | 관리자 계정이 없으면 계정 삭제 시 에러가 발생하는 문제 해결 |
| [SNR#1702](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1702) | 대시보드 그리드 위젯에서 경보 설정시 필드이름 매크로가 동작하지 않는 문제 해결 |
| [SNR#1980](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1980) | event 쿼리 명령어에 raw=t 옵션을 지정한 경우 티켓 조회 권한에 따른 필터링이 누락된 문제 해결 |
| [SNR#2175](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2175) | result, load 쿼리 명령어가 취소되지 않는 문제 및 쿼리 수행 중 브라우저 종료 시 웹 서버 스레드가 멈추는 문제 해결 |
| [SNR#2182](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2182) | 감사로그 화면에 로케일 설정이 적용되지 않는 문제 해결 |
| [SNR#2228](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2228) | 클러스터 환경에서 fulltext 쿼리 수행 시 클러스터 관리자 계정이 아닌 경우 다른 노드의 데이터를 가져오지 못하는 문제 해결 |
| [SNR#2242](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2242) | sonar 쿼리 명령어가 서브쿼리에서 동작하지 않는 문제 해결 |
| [SNR#2244](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2244) | datetrunc 함수의 timespan 인자를 0으로 입력하면 쿼리가 실패하는 문제 해결 |
| [SNR#2273](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2273) | 분산 환경에서 "fulltext \*:테이블" 유형의 쿼리문 수행 후 result 쿼리 커맨드로 결과 조회 시 에러가 발생하는 문제 해결 |
| [SNR#2282](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2282) | 시스로그 수집기의 정규식 필터 설정이 간헐적으로 적용되지 않는 문제 해결 |
| [SNR#2284](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2284) | 단일 노드 구성에서 fulltext 명령어에 대해 실행 계획 최적화가 동작하지 않던 문제 해결 |
| [SNR#2294](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2294) | 플레이북 명령어 "블랙리스트 추가"에 기간(분) 옵션 추가 |
| [SNR#2296](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2296) | 수집 노드가 여러 개인 환경에서 사용자 권한 계정이 서브쿼리의 클러스터 테이블 조회에 실패하는 문제 해결 |
| [SNR#2391](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2391) | 사용자 권한 계정이 자신의 정보 수정 시 '티켓 분류 권한 부여에 실패'했다는 메시지가 표시되는 문제 해결 |
| [SNR#2392](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2392) | 네트워크 대역 메뉴에서 설명이 표시되지 않는 문제 해결 |
| [SNR#2393](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2393) | 보고서 목록 화면에서 수정일이 생성일로 표시되는 문제 해결 |
| [SNR#2394](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2394) | 주소 그룹 화면에서 영문 로케일 일부가 한글로 표시되는 문제 해결 |
| [SNR#2395](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2395) | 플레이북에서 티켓 생성 태스크를 실행할 때 필수 매개변수만 입력하면 티켓 생성 실패하는 문제 해결 |

### 상세 내역

#### SNR#2138 앱 관리 기능 추가

웹 콘솔에서 로그프레소 앱을 관리할 수 있는 기능이 추가되었습니다.



**클러스터 단위의 앱 설치 및 제어**

이전 버전에서는 각 노드마다 일일이 앱을 설치해야 했으나, 이제 웹 콘솔에서 앱을 업로드하면 전체 클러스터 노드에 자동으로 앱이 설치됩니다. 앱을 삭제하면 클러스터의 모든 노드에서 자동으로 삭제됩니다. 마찬가지로, 웹 콘솔에서 앱을 활성화 또는 비활성화하면 클러스터의 모든 노드에서 앱이 활성화되거나 비활성화됩니다.

이제 JDBC 드라이버도 스토어를 통해 배포되며 앱으로 설치할 수 있습니다. 새 버전부터는 JDBC 드라이버를 설치하더라도 서비스를 재시작할 필요가 없습니다.

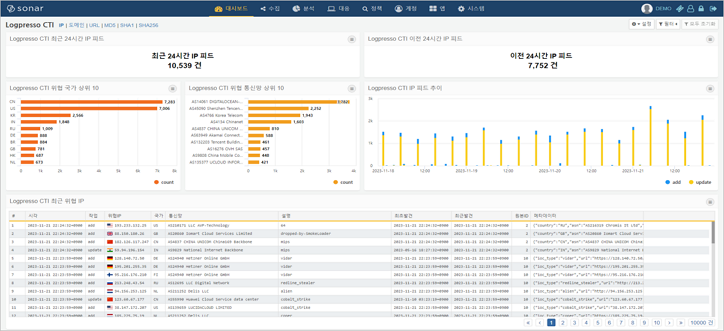
**앱 객체 자동 업데이트**

파서, 로그 스키마, 위젯, 대시보드, 패턴 그룹, 탐지 시나리오 등 앱을 통해 설치된 객체는 앱에 귀속됩니다. 각 객체는 고유한 GUID를 가지고 있으며 새 버전의 앱을 설치하면 자동으로 앱 객체가 업데이트됩니다.

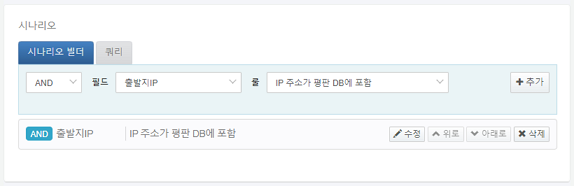
예를 들어 장비의 펌웨어가 업데이트되면 새로운 로그 유형이 추가되는 경우가 흔한데, 수집 설정을 일일이 변경하지 않아도 앱 업데이트만으로 관련된 설정이 자동으로 업데이트됩니다.

#### SNR#2046 CTI 침해지표 피드 추가

로그프레소 CTI 서비스에서 제공하는 위협 인텔리전스 피드가 추가되었습니다. 로그프레소 CTI 접속 프로파일에 API 키를 입력하여 생성하고, 위협 인텔리전스 피드 메뉴에서 로그프레소 CTI 피드를 활성화하면 아래와 같이 대시보드에서 CTI 피드 현황을 확인할 수 있습니다.



실시간 탐지 시나리오에서 아래와 같이 설정하면 대규모의 방화벽 로그에 대해서도 수천만 건의 침해지표(IoC, Indicator of Compromise)를 실시간으로 전수 검사할 수 있습니다.

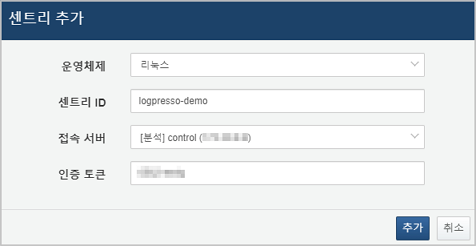


#### SNR#1503 센트리 자동 설치 및 인증서 관리 기능 추가

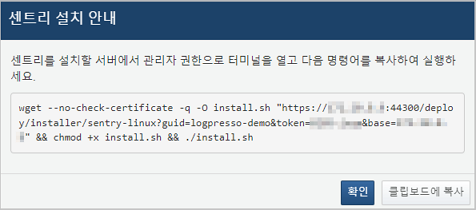
이전에는 로그프레소 센트리를 설치할 때 파일을 다운로드 받고 인증서를 설정하는 등 여러 단계의 작업을 수행해야 했습니다. 인증서도 openssl이나 keytool을 이용하여 직접 발급해야만 했고, 인증서 기간 만료 시 각 센트리의 인증서를 직접 교체해야 하므로 어려움이 있었습니다.

이제 웹 콘솔에서 서버와 센트리 인증서의 발급과 파기를 원 클릭으로 수행할 수 있으며, 화면에 표시되는 로그프레소 센트리 설치 명령어를 클립보드 복사 후 터미널에 붙여넣어 실행하는 간단한 작업으로 설치를 완료할 수 있습니다.

센트리 메뉴에서 추가 버튼을 클릭하면 아래와 같이 대화상자가 표시됩니다.



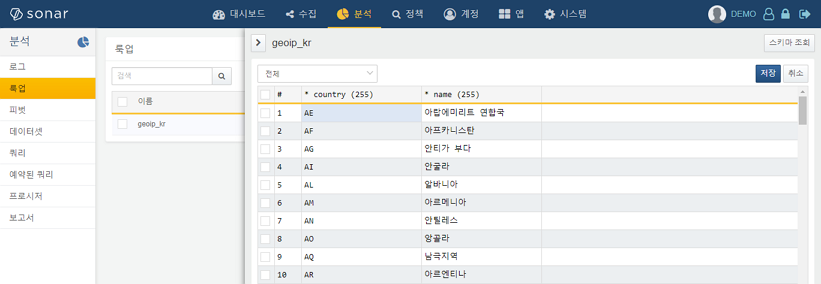
운영체제 종류를 선택한 후 센트리 ID에 유일한 호스트명을 입력하고 추가 버튼을 클릭합니다.



클립보드에 복사 버튼을 클릭하고 대상 서버에서 관리자 권한의 터미널에 명령어를 붙여넣어 실행하면 즉시 설치가 완료됩니다.

#### SNR#1812 룩업 기능 추가

새 룩업 기능이 추가되었습니다.



새 기능은 이전 세대 제품의 룩업과 아래의 측면에서 차이가 있습니다:

**클러스터 동기화**

이전에는 로그프레소 노드 단위로 룩업 데이터가 관리되었기 때문에 클러스터 환경에서 데이터 일관성을 유지하는데 어려움이 있었습니다. 이제 웹 콘솔에서 데이터를 편집하면 클러스터 전체에 자동으로 동기화됩니다.

**데이터량 제한 해제**

지금까지 JDBC 룩업 이외의 룩업 엔진은 힙 메모리에 모든 레코드를 유지했기 때문에 데이터 량에 한계가 있었습니다. 그러나 이제 디스크에 데이터를 유지하고 자주 참조되는 데이터를 캐시하는 방식으로 개선되어 100만 건 이상의 레코드도 문제 없이 처리할 수 있습니다.

**API를 통한 실시간 업데이트 지원**

일반적으로 룩업 데이터는 원본이 외부에 존재하므로 데이터를 동기화할 필요가 있습니다. 이전에는 주기적으로 룩업 데이터를 조회하여 동기화하기 때문에 변경사항이 뒤늦게 반영되는 한계가 있었습니다. 이제 룩업 REST API가 지원되므로 외부에서 룩업 데이터 변경이 발생할 때마다 실시간으로 동기화를 수행할 수 있습니다.

#### SNR#2065 예약된 쿼리 기능 추가

새 기능은 이전 세대 제품의 예약된 쿼리와 아래의 측면에서 차이가 있습니다:

**클러스터 단위의 실행**

이전에는 예약된 쿼리가 로그프레소 노드 단위로 실행되었기 때문에, 각 노드마다 예약된 쿼리를 설정해야만 하는 불편이 있었습니다. 새 기능은 클러스터의 특정 유형의 서버 집합에 대해 예약된 쿼리를 일괄 실행할 수 있습니다.

**워크플로우 지원**

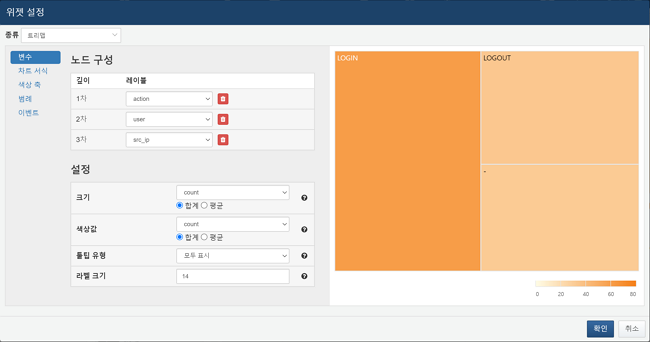
이전 세대의 제품은 예약된 쿼리와 워크플로우가 개별적인 기능이었습니다. 새 기능은 다른 예약된 쿼리의 완료, 성공, 실패에 따라 특정한 쿼리가 실행되도록 설정할 수 있으므로 더 직관적으로 동작합니다.

**실행 모니터링**

이전 세대의 제품은 쿼리 로그를 별도로 검색하지 않으면 예약된 쿼리가 언제 마지막으로 실행되었는지, 얼마나 소요되었는지 파악하기 어려웠습니다. 새 기능은 목록에서 쿼리 실행 상태를 바로 확인할 수 있습니다.

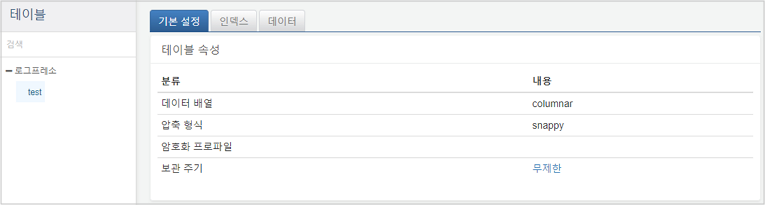
#### SNR#2144 트리맵 차트 위젯 유형 추가

위젯 유형에 트리맵 차트가 추가되었습니다. 각 항목 값의 크기에 따라 트리맵의 크기가 표시되며, 최대 3단계의 깊이를 가질 수 있습니다.



#### SNR#2222 테이블 보관 주기 수정 기능 추가

테이블 기본 설정 탭에 보관 주기 수정 기능이 추가되었습니다. 스토리지 엔진은 약 1시간 주기로 보관 주기가 지난 파티션을 자동으로 삭제합니다.



화면에서 보관 주기의 값을 클릭하면 대화상자가 표시되어 수정할 수 있습니다.

#### SNR#2264 lastindexof 함수 추가

문자열에서 특정 부분 문자열의 마지막 위치를 검색하는 [lastindexof()](https://docs.logpresso.com/ko/query/lastindexof-function) 함수가 추가되었습니다.

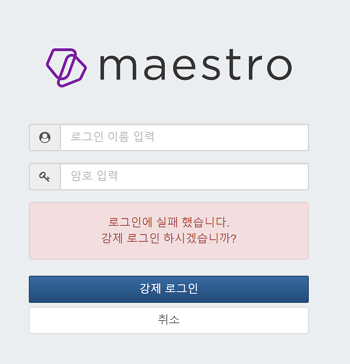
lastindexof(STR\_EXPR, SEARCH\_EXPR[, BEGIN\_EXPR])

#### SNR#1498 동일 계정 동시 접속 방지 기능 추가

동일 계정에 대해 동시 접속을 제한하는 옵션 BLOCK\_CONCURRENT\_LOGIN이 추가되었습니다. 다른 세션이 이미 접속되어 있는 경우 강제 로그인을 선택하여 기존에 접속되어 있던 세션을 끊고 접속할 수 있습니다.

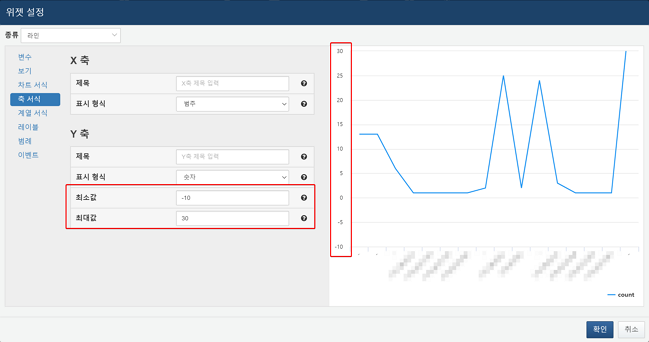
로그프레소 셸에서 다음과 같이 동시 접속 방지 옵션을 설정할 수 있습니다.

logpresso> sonar.setGlobalOption block\_concurrent\_login true



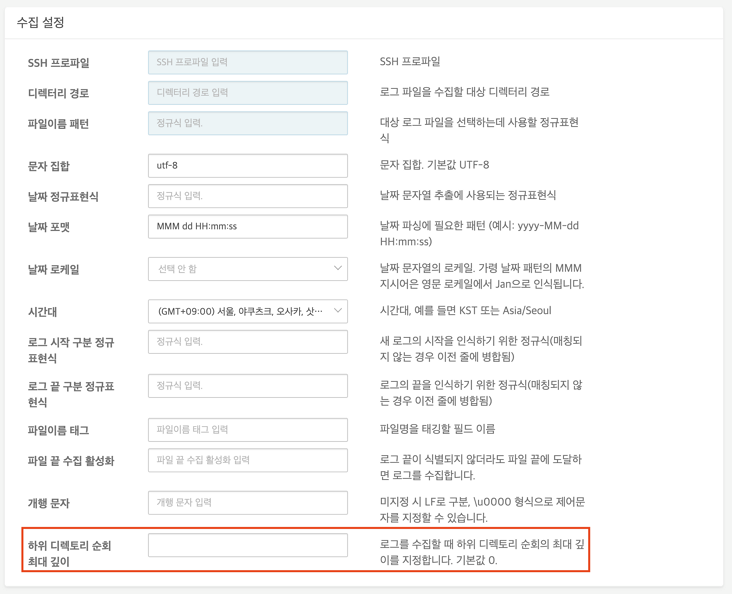
#### SNR#2148 위젯 종속 변수 최소값 및 최대값 옵션 추가

이제 위젯 설정에서 종속 변수에 대해 위젯에서 표시할 최소값과 최대값을 설정할 수 있습니다.



#### SNR#2173 SFTP 멀티 로테이션 수집기 하위 디렉토리 순회 기능 추가

SFTP 멀티 로테이션 로그 파일 수집 설정에 하위 디렉토리 순회 최대 깊이 옵션이 추가되었습니다. SFTP 서버의 특정 디렉토리 아래에서 파일이름 패턴과 일치하는 모든 로테이션 로그 파일을 수집할 수 있습니다.



#### SNR#2174 디렉토리 와처 수집기에 삭제된 파일의 수집 상태를 파기하는 옵션 추가

디렉터리 와처 유형 수집기에 삭제된 파일의 수집 상태를 파기할 수 있는 옵션이 추가되었습니다. -Daraqne.logapi.evict\_interval=MILLIS 시스템 스위치로 파일 삭제 여부 확인 주기를 설정하여 해당 기능을 활성화 할 수 있습니다.

(예시) 60초 주기마다 수집 파일 삭제 여부 확인

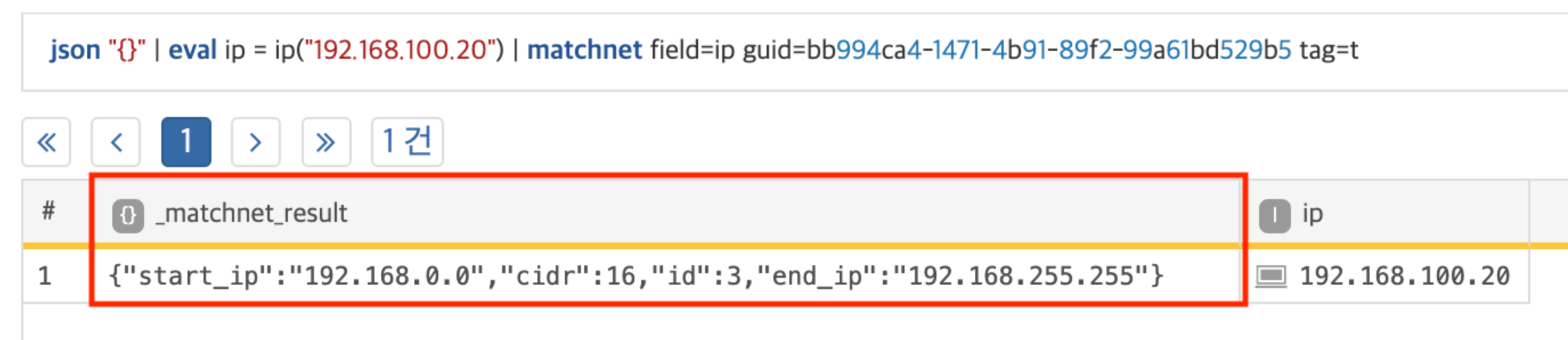
-Daraqne.logapi.evict\_interval=60000

해당 기능이 추가된 수집기 유형은 다음과 같습니다.

* 디렉터리 와처
* GZIP 디렉터리 와처
* 리커시브 디렉터리 와처
* PCAP 디렉터리 와처
* SFTP 디렉터리 와처

#### SNR#2177 matchnet 쿼리 명령어에 매칭 결과 필드를 반환하는 tag 옵션 추가

[matchnet 쿼리 커맨드](https://docs.logpresso.com/ko/query/matchnet-command)에 tag 옵션이 추가되었습니다. tag=t 옵션을 주면 매칭된 네트워크 대역에 대한 정보가 \_matchnet\_result 필드에 출력됩니다.



#### SNR#2227 JDBC 드라이버 플러그인 지원

기존에 내장되어 있던 JDBC 드라이버들을 플러그인화했습니다. 이전에는 JDBC 드라이버가 내장된 구조에서는 JDBC 드라이버를 업데이트해야 할 경우 패키지 전체를 업데이트해야 했습니다. 이 버전부터는 스토어에서 필요한 JDBC 드라이버 앱을 다운로드하여 설치하면 바로 사용할 수 있습니다.

MariaDB, MySQL, SQLite, Oracle 드라이버를 제외한 나머지 JDBC 드라이버들은 기본 패키징에서 제외했으며, 필요 시 로그프레소 스토어에서 해당 JDBC 드라이버 앱을 다운로드 받아 설치할 수 있습니다.

#### SNR#2237 사용자 정의 필터 변경 사항이 확률적으로 동기화되지 않는 문제 해결

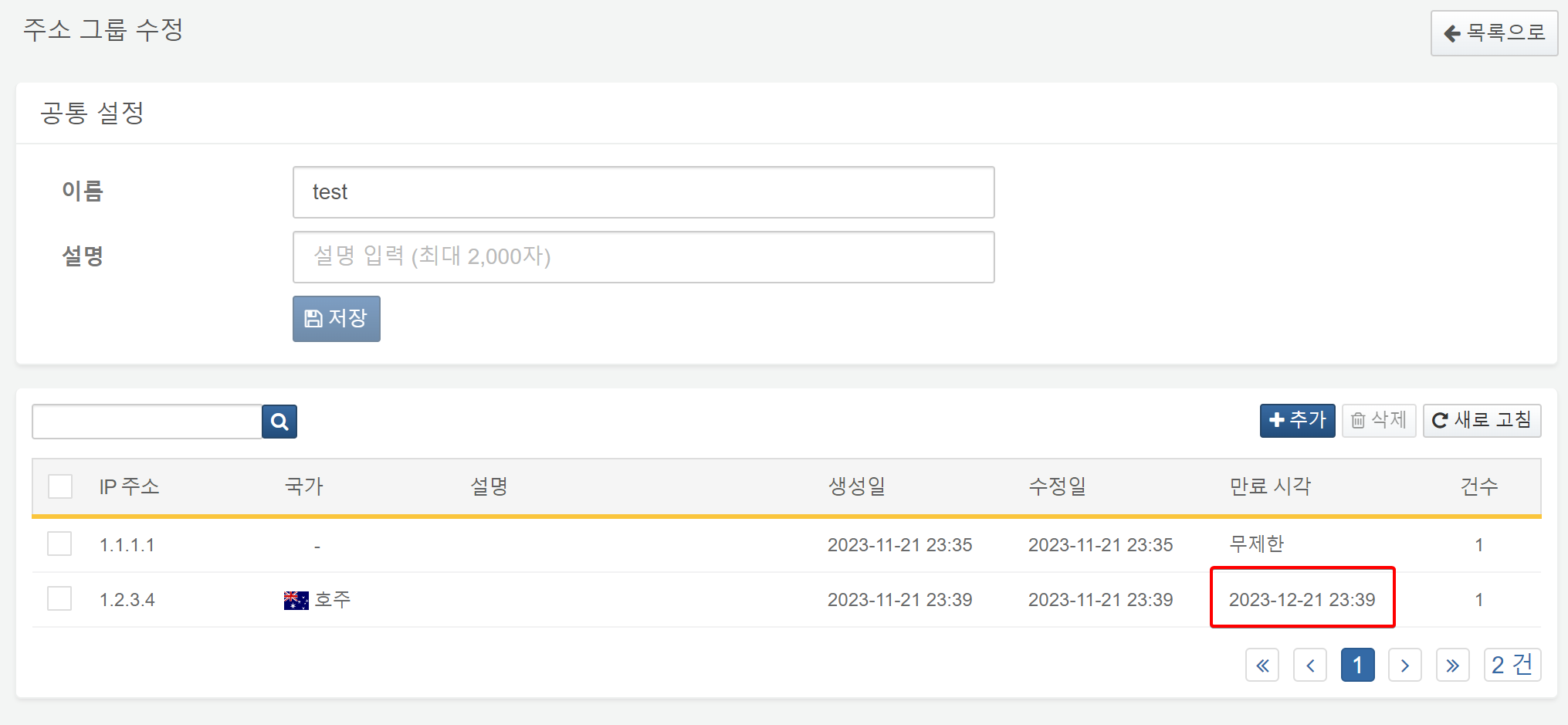
사용자 정의 필터 동기화 로직에서 테넌트 GUID를 참조하는 부분이 [SNR#2038 멀티 테넌트 기능 파기](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2038) 이슈 반영 시 수정되지 않아, 사용자 정의 필터에 대한 변경 사항이 확률적으로 적용되지 않던 문제가 해결되었습니다.

#### SNR#2267 sonar-add-address-batch 쿼리 명령어에 period 옵션 추가

sonar-add-address-batch 쿼리 명령어에 주소 만료 기한을 지정하는 period 옵션을 추가했습니다. 1~52560000분 사이의 값을 허용하고 미지정 시 무제한으로 설정합니다.

(예시) period 값을 43200분(30일)으로 설정

sonar-add-address-batch guid=e1de61d9-f112-493e-bbed-1c7d826effed period=43200



#### SNR#2274 대시보드 조회 시 불필요한 감사 로그 기록 제거

대시보드 화면 표시 중에 사용자 정의 변수 목록 조회 감사 로그가 반복적으로 기록되지 않도록 개선했습니다. 이는 불필요한 감사 로그의 기록으로 인해 감사 로그 조회 성능이 저하되는 문제를 해결합니다.

#### SNR#2275 iplookup 쿼리 명령어 성능 개선, company 옵션 필수 여부를 선택으로 변경

* iplookup 쿼리 명령어의 구현을 벡터화하여 성능을 개선했습니다.
* iplookup 쿼리 명령어에서 기존에 필수였던 company 옵션을 선택 옵션으로 변경했습니다.
* 멀티 테넌트 기능이 제거되면서 더 이상 테넌트 구분이 필요하지 않습니다.
* 배치 시나리오나 스트림 쿼리에서 iplookup 명령어에 company 옵션을 명시하지 않은 경우 쿼리가 실패하던 문제를 원천적으로 해결합니다.

#### SNR#2278 import 쿼리 명령어에서 create 옵션 제거

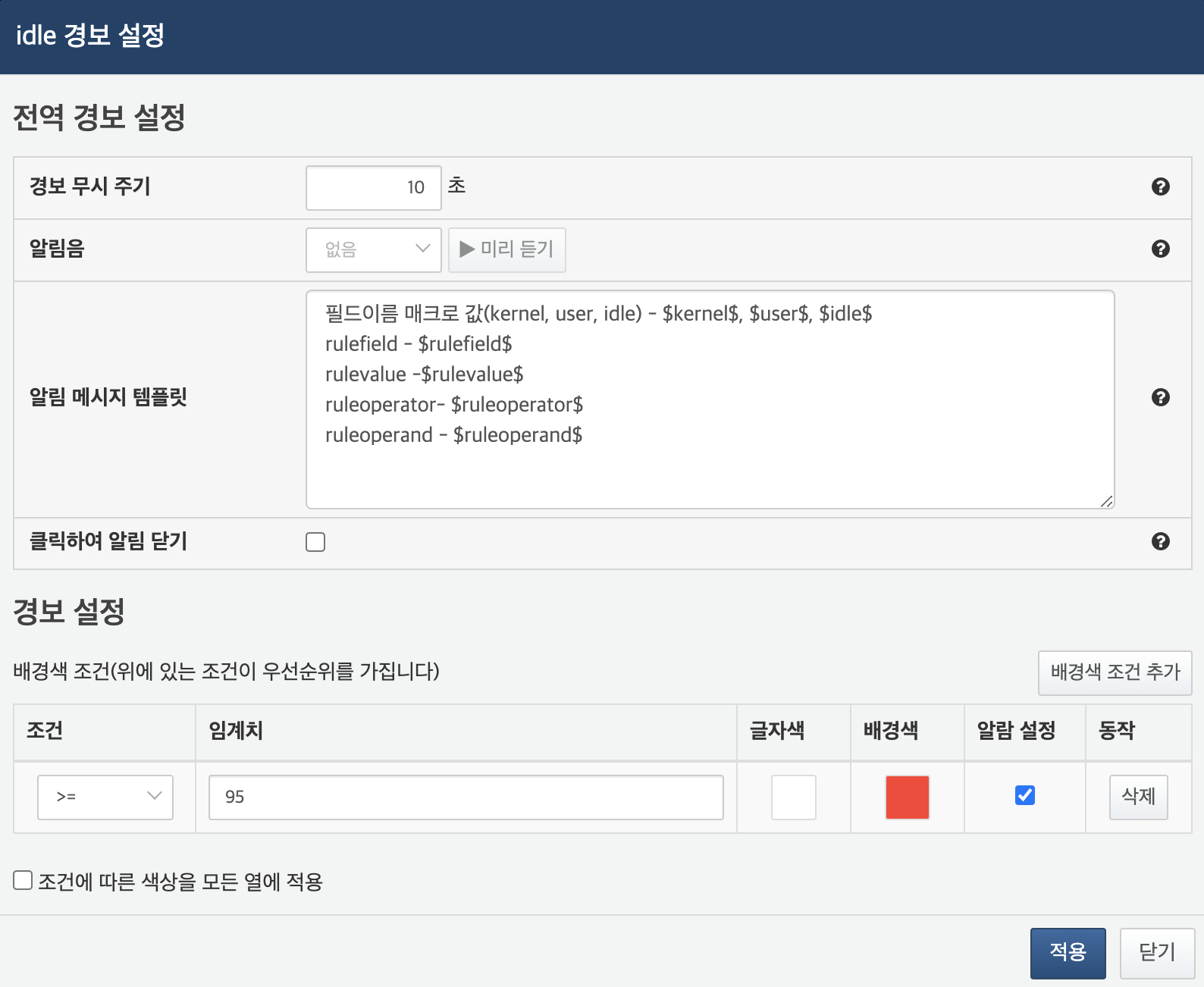
import 쿼리 명령어에서 create 옵션을 제거하였습니다. create 옵션으로 생성된 테이블은 엔터프라이즈 플랫폼에서만 사용 가능하고 소나 플랫폼에서는 인식되지 않으며 사용자 의도와 다른 기본값 설정으로 테이블을 생성하는 사례가 많아서 기능을 제거하였습니다. 이미 생성된 테이블에 대해 create=t 옵션을 사용한 경우에는 무시되므로 기존 세팅에서는 일반적으로 영향이 없습니다. 불가피한 경우 일시적으로 -Daraqne.logdb.import\_create\_option=enabled 시스템 스위치로 활성화 할 수 있습니다.

#### SNR#1240 관리자 계정이 없으면 계정 삭제 시 에러가 발생하는 문제 해결

계정 목록에 관리자 계정이 (클러스터 관리자 계정 제외) 존재하지 않으면 계정 삭제 시 "최소한 1개의 관리자 계정이 있어야 합니다." 라는 메시지의 에러가 발생하며 삭제에 실패하는 문제가 해결되었습니다.

#### SNR#1702 대시보드 그리드 위젯에서 경보 설정시 필드이름 매크로가 동작하지 않는 문제 해결

그리드 위젯에서 경보 설정 시 쿼리 매크로 중 $필드이름$ 매크로가 동작하지 않는 문제를 해결했습니다.



#### SNR#1980 event 쿼리 명령어에 raw=t 옵션을 지정한 경우 티켓 조회 권한에 따른 필터링이 누락된 문제 해결

* event 쿼리 명령어에 raw=t 옵션을 지정한 경우 결과가 티켓 분류 조회 권한에 따라 필터링되지 않고 모두 표시되던 문제가 해결되었습니다.
* 설치 시 이벤트 테이블에 인덱스가 자동으로 생성되지 않던 문제가 해결되었습니다.

#### SNR#2175 result, load 쿼리 명령어가 취소되지 않는 문제 및 쿼리 수행 중 브라우저 종료 시 웹 서버 스레드가 멈추는 문제 해결

* result, load 쿼리 커맨드가 취소되지 않는 문제를 해결했습니다.
* 쿼리가 수행 중일 때 브라우저를 닫으면서 세션이 종료된 경우, 웹 서버 스레드가 멈출 수 있는 문제를 해결했습니다.

#### SNR#2182 감사로그 화면에 로케일 설정이 적용되지 않는 문제 해결

계정 로케일 설정을 한국어에서 다른 언어로 변경해도 감사로그 화면에서는 로케일이 한국어로 표시되는 문제가 해결되었습니다.

#### SNR#2228 클러스터 환경에서 fulltext 쿼리 수행 시 클러스터 관리자 계정이 아닌 경우 다른 노드의 데이터를 가져오지 못하는 문제 해결

클러스터 환경에서 fulltext 쿼리 수행 시 쿼리를 수행한 계정이 클러스터 관리자 계정이 아닌 경우 다른 노드의 데이터를 가져오지 못하는 문제를 해결했습니다. 로그 화면 등에서 필터를 사용한 경우와 쿼리문에서 fulltext 커맨드 조회 대상에 타 노드의 테이블 데이터를 포함하는 경우 등이 문제 상황에 포함됩니다.

#### SNR#2242 sonar 쿼리 명령어가 서브쿼리에서 동작하지 않는 문제 해결

sonar 쿼리 명령어가 서브쿼리에서 동작하지 않는 문제가 해결되었습니다.

#### SNR#2244 datetrunc 함수의 timespan 인자를 0으로 입력하면 쿼리가 실패하는 문제 해결

datetrunc 함수의 두 번째 인자인 timespan 에 값을 0s, 0m, 0h 등 0을 입력했을 때 java.lang.ArithmeticException: / by zero 에러가 발생하면서 쿼리가 실패하는 문제가 있었습니다. 패치 후에는 timespan 인자에 0이 입력되면 시간 값을 원본 그대로 반환합니다.

#### SNR#2273 분산 환경에서 "fulltext \*:테이블" 유형의 쿼리문 수행 후 result 쿼리 커맨드로 결과 조회 시 에러가 발생하는 문제 해결

분산 환경에서 여러 노드를 대상으로 fulltext 쿼리문을 수행한 다음, result 쿼리 커맨드로 해당 쿼리의 결과를 조회하려 할 경우 NullPointerException 에러가 발생하던 이슈가 해결되었습니다.

* 쿼리문 예시

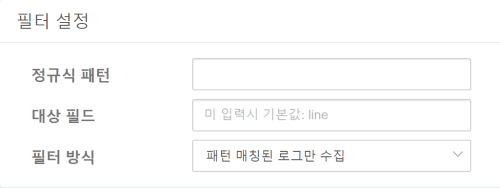
fulltext "TERM" from \*:table

* 에러 로그 예시

[2023-11-10 15:00:59.949] ERROR (QueryTaskRunner) - araqne logdb: query [20000304] task [query: 20000304 scan:result 19999434] failedjava.lang.RuntimeException: java.lang.NullPointerException at org.araqne.logdb.query.command.Result.run(Result.java:49) at org.araqne.logdb.DriverQueryCommand$ScanTask.run(DriverQueryCommand.java:45) at org.araqne.logdb.query.engine.QueryTaskRunner.run(QueryTaskRunner.java:57) at org.araqne.logdb.impl.QueryThreadPoolServiceImpl$NamedRunnable.run(QueryThreadPoolService Impl.java:129) at java.base/java.util.concurrent. ThreadPoolExecutor.runWorker (ThreadPoolExecutor.java:1128) at java.base/java.util.concurrent. ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:628) at java.base/java.lang.Thread.run(Thread.java:829)Caused by: java.lang.NullPointerException at com.logpresso.query.planner.DistributedFulltextLazyLoader.onLoad(DistributedFulltextLazyLoader.java:151) at com.logpresso.query.planner. DistributedFulltextLazyLoader.onLoad (DistributedFulltextLazyLoader.java:158) at org.araqne.logdb. LazyQueryResult$LazySink.process Logs (LazyQueryResult.java:138) at org.araqne.logstorage. LogTraverseCallback$Sink.write(LogTraverseCallback.java:157) at org.araqne.logstorage. LogTraverseCallback.writeLogs (LogTraverseCallback.java:51) at com.logpresso.logstorage.file.s.qzvc (SourceFile: 721) at com.logpresso.logstorage.file.s.qzvc (SourceFile: 792) at com.logpresso.logstorage.file.s.traverse (SourceFile:617) at org.araqne.logdb. LazyQueryResult.traverse(LazyQueryResult.java:102) at org.araqne.logdb.query.engine.QueryResultImpl.traverse (QueryResultImpl.java:258) org.araqne.logdb.query.command.Result.run(Result.java:46) ... 6 more

#### SNR#2282 시스로그 수집기의 정규식 필터 설정이 간헐적으로 적용되지 않는 문제 해결

시스로그 수집기의 정규식 설정이 확률적으로 적용되지 않아 일부 데이터가 필터링되지 않던 문제가 해결되었습니다.

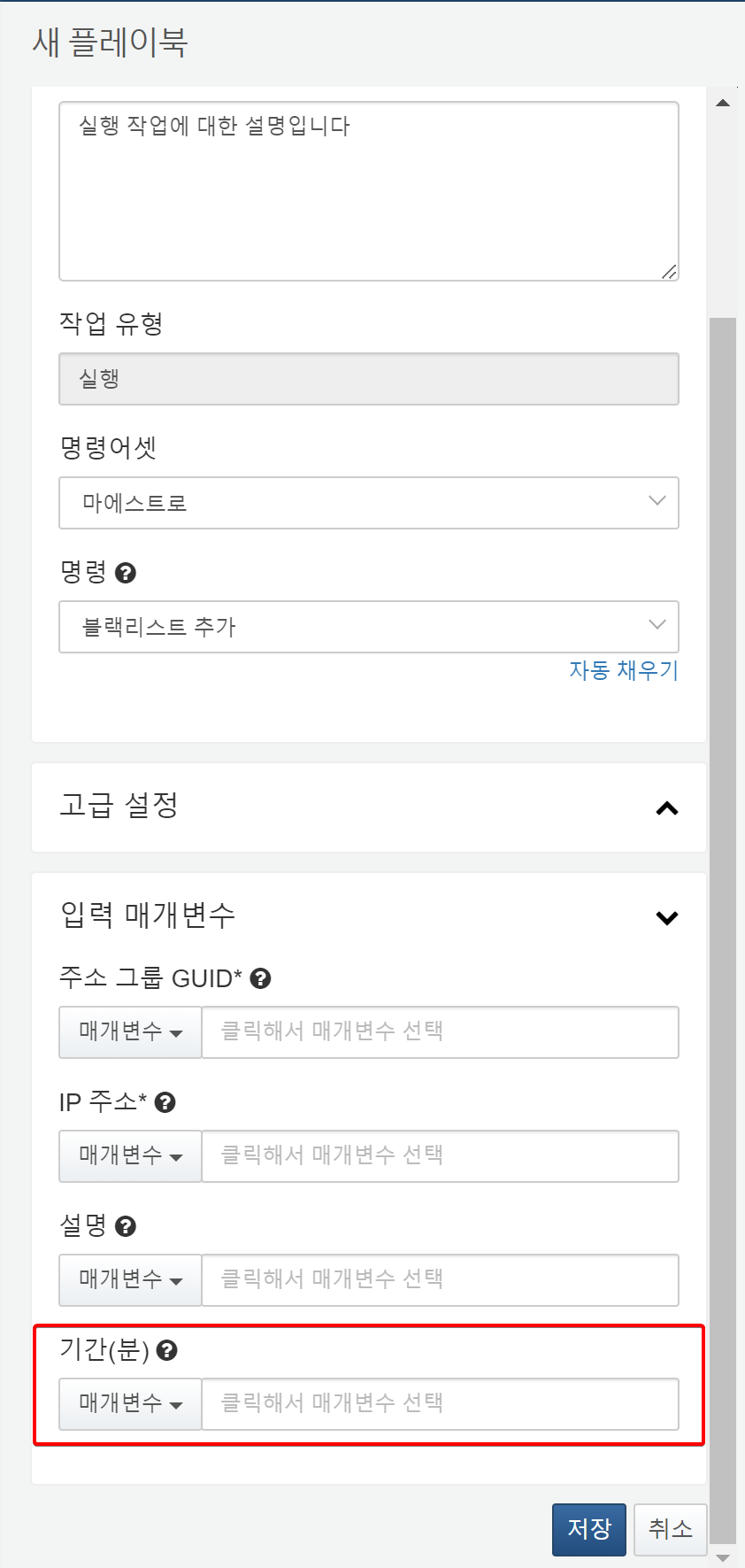


#### SNR#2284 단일 노드 구성에서 fulltext 명령어에 대해 실행 계획 최적화가 동작하지 않던 문제 해결

단일 노드 구성에서 fulltext 쿼리 명령어를 실행할 때, 실제 레코드를 조회하는 시점까지 테이블 접근을 지연시키는 실행 계획 최적화가 제대로 작동하지 않아 검색 성능이 느려지는 문제가 해결되었습니다.

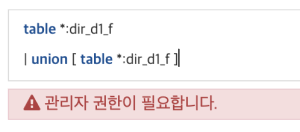
#### SNR#2294 플레이북 명령어 "블랙리스트 추가"에 기간(분) 옵션 추가

플레이북 명령어 "블랙리스트 추가"에 기간(분) 옵션이 추가되었습니다.



#### SNR#2296 수집 노드가 여러 개인 환경에서 사용자 권한 계정이 서브쿼리의 클러스터 테이블 조회에 실패하는 문제 해결

2개 이상의 수집 노드가 있는 환경에서 사용자 권한 계정으로 쿼리를 수행할 때, 서브쿼리에 클러스터 테이블 조회가 포함되어 있으면 쿼리 실행이 실패하는 문제를 해결하였습니다. 사용자에게 테이블 조회 권한이 있더라도 쿼리 창에서 '관리자 권한이 필요합니다'라는 메시지가 나타나며 실패합니다.



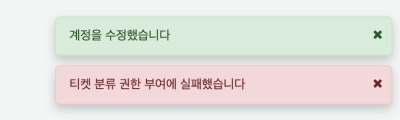
문제가 발생하는 쿼리 예시는 다음과 같습니다.

| union [ table \*:TABLE\_NAME ]

#### SNR#2391 사용자 권한 계정이 자신의 정보 수정 시 '티켓 분류 권한 부여에 실패'했다는 메시지가 표시되는 문제 해결

사용자 권한 계정이 자신의 정보 수정 시 수정 사항과 관련 없는 '티켓 분류 권한 부여에 실패' 메시지가 표시되는 문제를 해결했습니다.

패치 전에도 계정 정보 수정은 정상적으로 수행되었습니다.



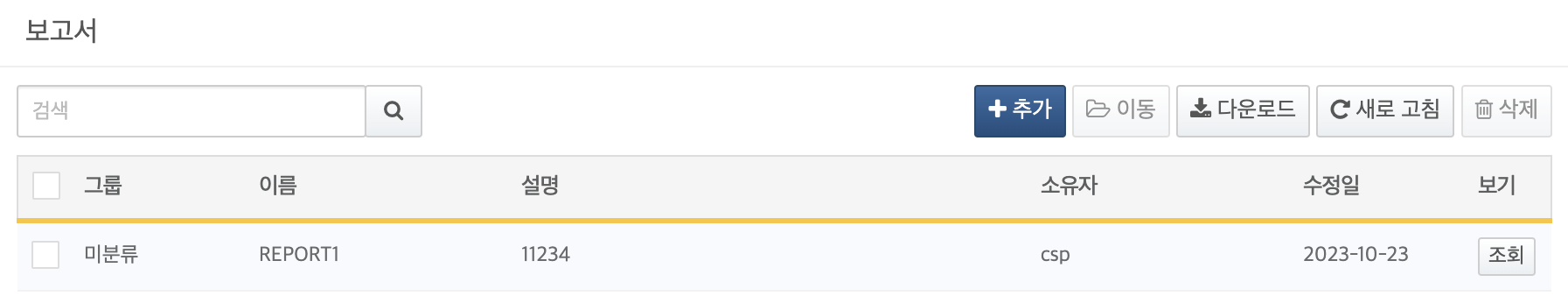
#### SNR#2392 네트워크 대역 메뉴에서 설명이 표시되지 않는 문제 해결

네트워크 대역 메뉴에서 설명 항목이 표시되지 않는 문제를 해결했습니다.

설명 자체는 정상적으로 저장되어 있었으며 화면에서 표시가 되지 않던 현상이었습니다.

#### SNR#2393 보고서 목록 화면에서 수정일이 생성일로 표시되는 문제 해결

보고서 목록 화면에서 수정일이 생성일이라고 표시되던 문제를 해결했습니다.



#### SNR#2394 주소 그룹 화면에서 영문 로케일 일부가 한글로 표시되는 문제 해결

주소 그룹 수정 화면에서 "유지 기간(분)" 항목이 한글로 표시되고 Add, Close 버튼 위치가 아랫줄로 밀리는 문제를 해결했습니다.

#### SNR#2395 플레이북에서 티켓 생성 태스크를 실행할 때 필수 매개변수만 입력하면 티켓 생성 실패하는 문제 해결

플레이북 티켓 생성 태스크 실행 시 필수 매개변수인 티켓 저장소 GUID, 티켓 제목 값만 입력하고 선택 매개변수들에 대해선 입력하지 않으면 티켓 생성에 실패하는 문제를 해결했습니다.