## 릴리스 4.0.2404.0

### 업그레이드 주의사항

* araqne-core 버전이 4.0.1로 업데이트되었습니다.
* TCP 18443 포트가 새로 개방되어 소명 전용으로 사용됩니다. 기존 웹 포트의 소명 접수 기능은 유지되지만 가능한 경우에는 웹 포트를 분리하여 보안을 강화할 것을 권고합니다. 자세한 내용은 [SNR#2286](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2286)를 참조하세요.
* 인사 정보를 임직원 객체에 자동으로 동기화하는 경우, sonar\_employees 테이블의 locale 컬럼에 로케일 값(한국어: ko, 영어: en, 중국어: zh)이 꼭 들어가도록 수정하세요. locale 컬럼은 소명 요청/검토 및 로그 스키마의 국제화(SNR#2239)에서 사용되는 컬럼으로, locale 값이 null이면 소명 프로세스가 정상 동작하지 않습니다.

### 핵심 기능

|  |  |
| --- | --- |
| 식별자 | 항목 |
| [SNR#2070](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2070) | 전달 노드를 통한 자동 부하 분산 지원 |
| [SNR#2157](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2157) | 스토리지 생명주기 웜 티어 추가 및 WORM 스토리지 지원 |
| [SNR#2239](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2239) | 소명 요청/검토 및 로그 스키마의 국제화 |
| [SNR#2291](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2291) | OTP 기반 2단계 인증 지원 |

### 신규 기능

|  |  |
| --- | --- |
| 식별자 | 항목 |
| [SNR#1541](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1541) | 디스크 고갈 대응 설정 추가 |
| [SNR#1542](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1542) | 시스템 로그 메뉴 추가 |
| [SNR#2097](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2097) | percentile(), median() 집계 함수 추가 |
| [SNR#2143](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2143) | 대시보드 외부 게시 기능 및 대시보드 게시 전용 계정 유형 추가 |
| [SNR#2178](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2178) | 쿼리 자동완성 단축키 추가 |
| [SNR#2233](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2233) | 로그 메뉴에 날짜/시간 값에 대한 필터 추가 |
| [SNR#2254](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2254) | 수집기 REST API 지원 |
| [SNR#2255](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2255) | 프로시저 REST API 지원 |
| [SNR#2280](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2280) | parsejson 쿼리 명령어 flatten, cutoff, lenient 옵션 추가 |
| [SNR#2281](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2281) | 사용자 정의 필터 화면에 AND/OR 그룹 트리 UI 추가 |
| [SNR#2287](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2287) | 보고서 메일 전송 쿼리 명령어 sonar-send-report 추가 |
| [SNR#2307](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2307) | 룩업 스키마 필드 길이 제약 완화 |
| [SNR#2309](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2309) | 시스로그 TCP 전송 쿼리 명령어 sendsyslog-tcp 추가 |
| [SNR#2432](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2432) | system logs 쿼리 명령어에 tail 옵션 추가 |

### 변경 내역

#### 엔진

|  |  |
| --- | --- |
| 식별자 | 항목 |
| [SNR#2172](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2172) | 인덱스 토큰 최대 길이를 255자로 제한 |
| [SNR#2265](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2265) | 패턴 그룹에 패턴 대량 등록 시 시스템 부하가 생기는 문제 해결 |
| [SNR#2293](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2293) | TCP 시스로그 서버에서 수신 오류 시 파일 누수가 발생하는 문제 해결 |
| [SNR#2344](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2344) | 특정 조건에서 행위 프로파일 동기화가 지연되는 문제 해결 |
| [SNR#2367](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2367) | TCP 시스로그 서버에서 파일 누수가 발생하는 문제 해결 |
| [SNR#2375](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2375) | TCP 443 포트에 웹 콘솔 바인딩 실패 시 재시도 포트 번호를 4443으로 변경 |
| [SNR#2379](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2379) | 동일 일자 시스템 로그 파일을 두 번째 순환할 때 부팅이 불가능한 문제 해결 |
| [SNR#2383](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2383) | 분석 노드 설치 시 티켓 감사 로그 테이블의 이중화 설정 누락 해결 |
| [SNR#2385](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2385) | 테이블 백업, 복원 시 메모리 누수 문제 해결 |
| [SNR#2389](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2389) | 앱 재설치 시 앱 부속 모듈이 재설정되지 않던 문제 해결 |
| [SNR#2402](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2402) | 윈도우 서버 2016, 2012에서 센트리 자동 설치가 동작하지 않는 문제 해결 |
| [SNR#2429](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2429) | 예약된 쿼리 실행 실패 시 오류 메시지가 255자를 초과하면 예약된 쿼리 상태가 변경되지 않는 문제 해결 |
| [SNR#2436](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2436) | CentOS 7 서버에서 센트리 자동 설치가 실패하는 문제 해결 |
| [SNR#2440](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2440) | 인덱스 생성 시 블룸필터 활성화 |
| [SNR#2470](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2470) | sonar-node 번들 재시작 시 소나 웹 콘솔 접속 등 일부 기능이 동작하지 않는 문제 해결 |

#### 쿼리

|  |  |
| --- | --- |
| 식별자 | 항목 |
| [SNR#2088](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2088) | nvl 함수 호출 시 원본 필드 변경 문제 해결 |
| [SNR#2354](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2354) | sonar-export-report 쿼리 명령어의 PDF 파일 생성 지원 |
| [SNR#2362](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2362) | 0 이하의 데이터에 대한 최댓값이나 양의 무한대 데이터에 대한 최솟값을 잘못 계산하는 문제 해결 |
| [SNR#2363](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2363) | 특정한 상황에서 sort, stats 쿼리 명령문이 by로 끝나는 필드명을 잘못 파싱하는 문제 해결 |
| [SNR#2378](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2378) | 쿼리 ID가 2,147,483,647를 초과하는 경우 쿼리 파싱에 실패하는 문제 해결 |
| [SNR#2400](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2400) | result 쿼리 명령어 성능 복원 |
| [SNR#2409](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2409) | 특정 테이블을 대상으로 동시에 purge 쿼리문 실행 시 낮은 확률로 해당 테이블에 쓰기 잠금이 해제되지 않는 문제 해결 |
| [SNR#2449](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2449) | setq dbquery 형태의 쿼리가 실패하는 문제 해결 |
| [SNR#2453](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2453) | 분산 쿼리 시 쿼리 종료와 쿼리 결과 처리 스레드가 확률적으로 경쟁하며 메모리가 누수되는 문제 해결 |

#### 대시보드

|  |  |
| --- | --- |
| 식별자 | 항목 |
| [SNR#2352](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2352) | 파이 차트 생성 시 "독립 변수와 종속 변수를 설정해야 합니다." 메시지가 출력되며 생성 실패하는 문제 해결 |
| [SNR#2472](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2472) | 파이 차트 클릭 이벤트에서 $필드이름$ 매크로 값이 잘못 매핑되는 문제 해결 |

#### 수집

|  |  |
| --- | --- |
| 식별자 | 항목 |
| [SNR#2167](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2167) | 수집기가 수천 개 이상일 때 수집기 목록 화면에 부하가 걸리는 문제 해결 |
| [SNR#2230](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2230) | 파서 목록 이동 시 기존 검색어 및 페이지 번호 유지 |
| [SNR#2251](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2251) | 수집기 편집 화면에서 값이 없는 항목에 대해 기본값을 표시하는 문제 해결 |
| [SNR#2271](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2271) | 파서 설정에 입력 가능한 문자열 길이 제한 추가 |
| [SNR#2315](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2315) | PCAP 디렉터리 와처 수집기가 payload 항목 수집을 누락하는 문제 해결 |
| [SNR#2325](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2325) | SNMP 인터페이스 통계 수집기가 1개만 동작하는 문제 해결 |
| [SNR#2411](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2411) | 수집 모델에서 사용 중인 로그 스키마 삭제 시도 시 오류 메시지를 명확하게 표시하도록 수정 |

#### 티켓

|  |  |
| --- | --- |
| 식별자 | 항목 |
| [SNR#1477](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1477) | 티켓 첨부 파일 삭제 불가 및 미리보기 깨짐 문제 해결, 크기 15MB 제한 |
| [SNR#2176](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2176) | 중복 티켓 축약 시 변경되지 않아야 할 값들이 수정되는 문제 해결 |
| [SNR#2240](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2240) | 티켓 직접 생성 시 생성자가 시스템으로 잘못 표시되는 문제 해결 |
| [SNR#2313](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2313) | 반려된 티켓의 상태 변경이 불가능한 문제 해결 |
| [SNR#2326](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2326) | 티켓이 대량 발생한 날짜 범위에 대해 태그 검색 시 성능이 저하되는 문제 해결 |
| [SNR#2358](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2358) | 티켓 제목이 255자를 초과하면 티켓 생성이 실패하는 문제 해결 |
| [SNR#2433](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2433) | 플레이북으로 생성된 티켓의 태스크 탭 조회 시 새로고침 주기마다 화면이 위로 이동하는 문제 해결 |
| [SNR#2441](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2441) | 티켓 생성 REST API 호출 시 NullPointerException 예외 발생하며 실패하는 문제 |
| [SNR#2471](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2471) | 티켓 태그를 수정하는 REST API 및 플레이북 명령 추가 |

#### 소명

|  |  |
| --- | --- |
| 식별자 | 항목 |
| [SNR#1878](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1878) | 소명 요청 화면 사용자 인터페이스 개선 |
| [SNR#1953](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1953) | 티켓에 대한 소명 요청 시 대상자 자동 할당 |
| [SNR#1954](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1954) | 소명 화면에 소명 요청자, 검토자 표시 |
| [SNR#1983](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1983) | 메일 서버 설정을 누락한 상태에서 소명 메일 발송 시 NullPointerException 예외 발생하는 문제 해결 |
| [SNR#1998](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1998) | 자동/수동 소명 마감시한을 자정으로 통일 |
| [SNR#2286](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2286) | 소명 전용 웹 포트 분리 |
| [SNR#2308](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2308) | 소명 조회 시 행위 기간에 티켓 탐지 일시가 잘못 표시되는 문제 해결 |
| [SNR#2349](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2349) | 소명 요청 화면의 임직원 선택 창에서 부서 트리를 최상위 단계로 축소 표시하도록 수정 |
| [SNR#2446](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2446) | 임직원 선택 창에 부서 검색 창 추가 |

#### 정책

|  |  |
| --- | --- |
| 식별자 | 항목 |
| [SNR#1833](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1833) | 실시간 탐지 시나리오 빌더 개선 |
| [SNR#2015](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2015) | 웹 콘솔에서 패턴 추가 시 유효성 검사 수행 |
| [SNR#2181](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2181) | 머신러닝 모델 내보내기/불러오기 기능 추가 |
| [SNR#2231](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2231) | 자산 IP 목록 다운로드 시 사이트 항목 필터가 반영되지 않는 문제 해결 |
| [SNR#2312](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2312) | 시나리오 분류 관리 메뉴에 삭제 버튼 추가 |
| [SNR#2370](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2370) | 배치 시나리오 실행 시 표시되지 않던 오류 로그 추가 |
| [SNR#2410](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2410) | 알람 그룹에 계정 그룹을 하나만 할당해도 모든 계정 그룹이 할당된 것으로 보이는 문제 해결 |
| [SNR#2419](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2419) | 실시간 탐지 시나리오 목록에서 분류 필터가 동작하지 않는 문제 해결 |
| [SNR#2477](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2477) | 실시간 시나리오 불러오기가 실패하는 문제 해결 |

#### 플레이북

|  |  |
| --- | --- |
| 식별자 | 항목 |
| [SNR#2322](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2322) | 실행 중인 플레이북 수정 시 자동 대응 내역 및 티켓 태스크 조회, 승인 동작이 실패하는 문제 해결 |
| [SNR#2376](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2376) | 플레이북 목록에서 "시작 유형"이 새 사이트로 표시되는 문제 해결 |
| [SNR#2420](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2420) | 플레이북 관련 버그 및 개선 사항 |
| [SNR#2426](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2426) | 플레이북 사용자 입력 태스크의 유효성 검사 옵션 추가 |
| [SNR#2428](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2428) | 플레이북 태스크 "실패 허용" 옵션 추가 |
| [SNR#2454](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2454) | 플레이북 분기 태스크에 불리언이 아닌 표현식을 사용할 때 NullPointerException 예외 발생하는 문제 해결 |

#### 계정

|  |  |
| --- | --- |
| 식별자 | 항목 |
| [SNR#1976](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1976) | 암호 만료 기한을 7일로 설정하면 암호 변경을 해도 암호 변경 창이 계속 뜨는 문제 해결 |
| [SNR#2220](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2220) | 계정 추가 화면에서 역할 기본값을 사용자로 변경 |
| [SNR#2226](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2226) | 사용자 권한 계정은 타 계정의 최소 정보만 접근하도록 보안 강화 |
| [SNR#2377](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2377) | 로그인 계정 이름에 . 문자를 허용하도록 수정 |
| [SNR#2403](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2403) | 관리자 권한으로 클러스터 관리자 계정 삭제 시도 시 삭제 실패임에도 성공 메시지가 출력되는 문제 해결 |

#### 시스템

|  |  |
| --- | --- |
| 식별자 | 항목 |
| [SNR#2272](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2272) | 센트리 접속 상태 아이콘이 단절 상태(회색)에서 변경되지 않는 문제 해결 |
| [SNR#2348](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2348) | 메일 서버 프로토콜이 포트 번호에 따라 결정되는 문제 해결 |
| [SNR#2366](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2366) | 접속 프로파일, 인증서 관련 웹 콘솔 메시지 수정 |
| [SNR#2401](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2401) | 차단 연동 세부설정 화면에서 드롭다운 항목의 표시 이름과 값이 뒤바뀌는 문제 해결 |
| [SNR#2434](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2434) | 성능 모니터에서 각 지표의 시간 차가 항상 0초로 표시되는 문제 해결 |
| [SNR#2448](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2448) | 설치 직후 테이블 메뉴 조회 시 NullPointerException 발생하는 문제 해결 |
| [SNR#2451](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2451) | 최초 설치 시 클러스터 노드의 인증서 검증 설정이 활성화되는 문제 해결 |
| [SNR#2456](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2456) | 성능 모니터에서 GC 지표 문구 수정 |

#### 기타

|  |  |
| --- | --- |
| 식별자 | 항목 |
| [SNR#1463](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1463) | 웹 콘솔 GNB에 제품 버전 정보 표시 |
| [SNR#1690](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1690) | 수집기, 예약된 쿼리, 배치 시나리오 일정 입력 시 긴 입력값 및 복합 일정 입력 지원 |
| [SNR#2248](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2248) | 제품 전반에 걸친 웹 콘솔 사용성 개선 및 버그 수정 |
| [SNR#2250](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2250) | 객체 생성 및 편집 시 입력값 유효성 검증 개선 |
| [SNR#2371](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2371) | 잘못된 쿠키 값이 설정된 경우 로그인 후 브라우저 새로고침 시 다시 로그인 창이 출력되는 문제 해결 |
| [SNR#2417](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2417) | 쿠키 탈취 시도 시 NullPointerException 예외가 발생하는 문제 해결 |
| [SNR#2425](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2425) | REST API 경로에 포함된 매개변수가 URL 디코드 되지 않는 문제 해결 |
| [SNR#2431](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2431) | 날짜 선택기에서 1월 이전이나 12월 이후로 이동해도 연도가 바뀌지 않는 문제 해결 |

### 상세 내역

#### SNR#2070 전달 노드를 통한 자동 부하 분산 지원

**개요**

전달 노드는 새로 추가된 클러스터 노드 유형으로, 로그프레소 소나의 고가용성과 부하분산 기능을 강화하는 역할을 수행합니다.

전달 노드는 수집 노드의 앞에 배치되어 로그프레소 소나 클러스터가 수신하는 모든 데이터의 게이트웨이처럼 동작합니다. 수집 노드에 장애가 발생하면 전달 노드는 자신의 메모리와 디스크를 사용해 아직 수집 노드에 적재 완료되지 않은 데이터를 보관합니다. 수집 노드가 복구되면 전달 노드는 보관 중인 데이터를 수집 노드에 전송함으로써 고가용성을 향상시킵니다. 또한 수집한 데이터를 각 수집 노드 페어에 균등하게 분배(라운드-로빈)하여 전송하여 부하를 분산합니다.

**적재와 수집의 분리**

이전 버전에서는 수집기와 데이터가 적재되는 위치가 같은 클러스터 노드이어야만 했지만, 4.0.2404.0 버전부터 수집기를 운영 위치가 전달 노드로 변경되었습니다. 이에 따라 수집기 생성 시 설정해야 하는 '수집 노드'는 '적재 위치'로, '센트리'는 '수집 위치'로 명칭이 변경되었습니다.

4.0.2404.0 버전으로 업그레이드하더라도 수집기 설정에 대한 하위 호환성을 보장합니다. 전달 노드가 구성된 환경에서는 수집기를 전달 노드에 생성하는 것이 권장되지만, 수집 노드, 센트리에 수집기를 생성, 운영할 수 있습니다. 2404.0 버전으로 업그레이드하기 전에 이미 사용하던 기존 수집기들은 그대로 유지됩니다. 기존 수집기를 전달 노드로 옮겨 생성하고자 하는 경우, 수집 위치를 바꿔서 새 수집기를 구성해야 합니다.

전달 노드가 구성된 환경에서 센트리는 전달 노드로 수집된 데이터를 전송하도록 구성을 변경하는 것이 좋습니다. 기존 구성을 유지하는 것도 가능하지만, 전달 노드에 연결시켜야 부하분산과 고가용성의 이점을 누릴 수 있습니다.

**부하 분산 적용**

전달 노드에 생성된 수집기나 전달 노드에 연결된 센트리에 위치한 수집기로부터 수집된 데이터는, 전달 노드의 부하분산 기능을 이용하여 전체 수집 노드 세트에 데이터를 고르게 분산하여 처리 및 적재할 수 있습니다.

이번 버전에서는 부하분산시 데이터의 위치를 결정짓는 파티셔닝 알고리즘은 라운드-로빈 방식만 지원합니다. 향후 다양한 방식의 파티셔닝 방식을 지원할 계획입니다.

**전달 노드 추가 구성**

로그프레소 클러스터를 구성할 때 전달 노드가 반드시 필요한 것은 아닙니다. 새로운 클러스터를 구성할 때 이전 버전에서와 같이 분석 노드, 수집 노드만 사용하는 클러스터를 구성하는 것도 가능합니다.

전달 노드를 기존 구성에 추가하고자 하는 경우, 권장되는 하드웨어 사양은 전체 노드에 대한 수집 용량에 따라 다르기 때문에, 제안/구축 담당자와 협의해주세요.

**전달 노드 장애 대응**

전달 노드는 효과적인 고가용성 달성을 위해 액티브-액티브 방식으로 동작합니다. 두 대 서버를 이용해 이중화된 전달 노드를 구성하면 한 대에 장애가 발생하더라도, 다른 한 대에서 별도의 절체과정 없이 데이터 수집/전송이 이뤄집니다.

전달 노드에 구성된 수집기 또한 액티브-액티브 개념에 맞게 동작합니다. 시스로그 수집기처럼 데이터 수집 시 상태 관리가 필요하지 않은 패시브 방식 수집기는 모든 전달 노드에서 수집기가 동시에 동작합니다.

그러나 수집 상태 관리가 요구되는 SFTP 혹은 JDBC 수집기의 경우, 이중화된 전달 노드 중 임의의 노드 한대에서 수집기가 동작합니다. 전달 노드 중 한 대에 장애가 발생하면 다른 전달 노드로 수집기 동작 위치가 자동으로 변경되고, 마지막 수집 상태도 자동으로 동기화됩니다.

#### SNR#2157 스토리지 생명주기 웜 티어 추가 및 WORM 스토리지 지원

스토리지 생명주기에 핫(hot) 티어와 콜드(cold) 티어 사이에 웜(warm) 티어 설정 기능이 추가되었습니다. 웜 티어는 핫 노드 페어와 동일한 구성으로 데이터를 저장합니다.

데이터 저장만 되고 이동이나 삭제가 불가능한 WORM 스토리지를 웜(warm) 티어에 설정할 수 있는 기능이 추가되었습니다.

티어 설정은 분석 노드의 로그프레소 셸에서 sonar.setGlobalOption 명령으로 설정할 수 있습니다. sonar.setGlobalOption 명령에 추가된 스토리지 생명주기 옵션은 다음 표를 참조하세요.

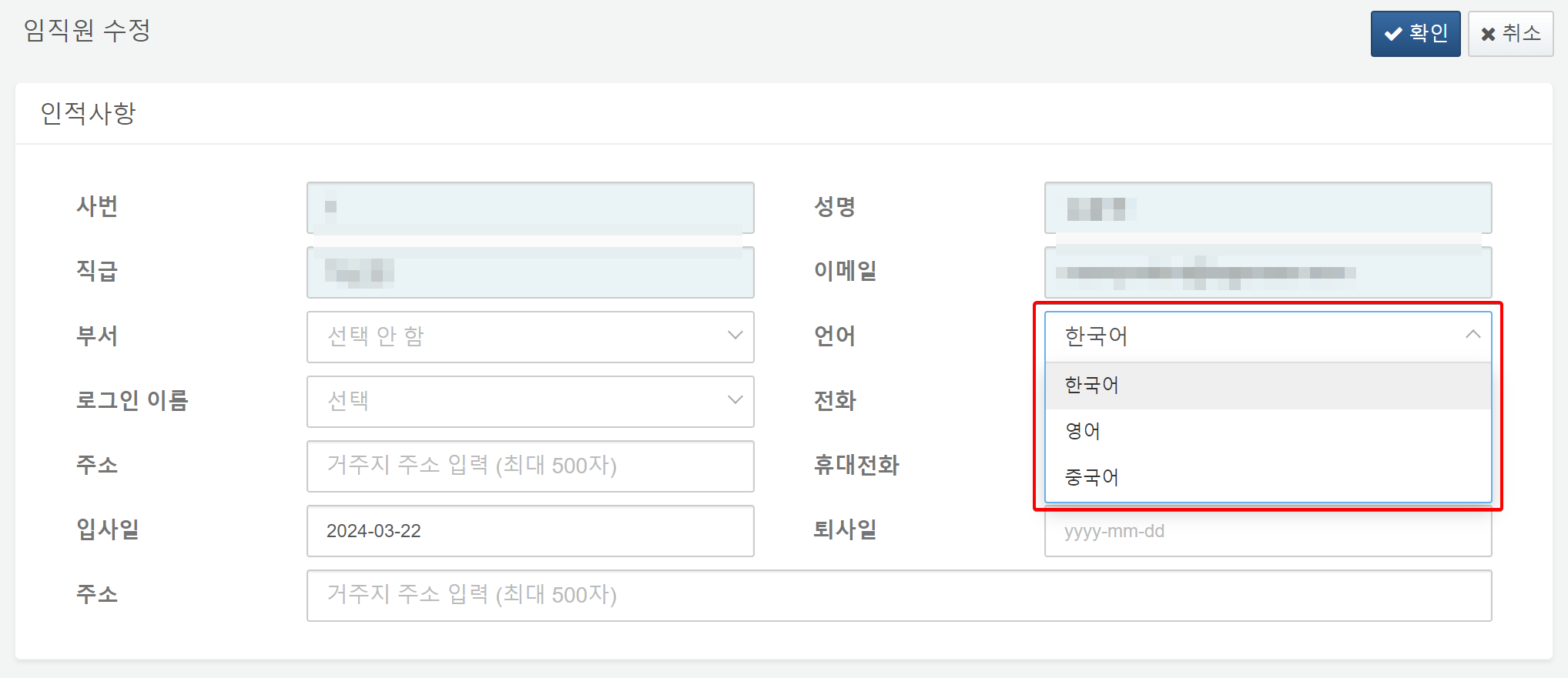
|  |  |  |
| --- | --- | --- |
| 옵션명 | 설명 | 설정값 예시 |
| lifecycle\_path\_warm | 웜 티어 경로 | sonar.setGlobalOption lifecycle\_path\_warm /warm |
| lifecycle\_retention\_warm | 웜 티어 생명주기(단위:일) | sonar.setGlobalOption lifecycle\_retention\_warm 120 |
| lifecycle\_worm\_warm | 웜 티어의 WORM 스토리지 여부 | sonar.setGlobalOption lifecycle\_worm\_warm true |

#### SNR#2239 소명 요청/검토 및 로그 스키마의 국제화

임직원 정보에 언어 설정이 추가됨에 따라, 임직원 정보 자동 연동을 하고 있는 경우 sonar\_employees 테이블에 locale 컬럼도 추가하고 동기화해야 합니다. 임직원의 언어가 한국어일 때 "ko", 영어 "en", 중국어 "zh"을 지정하세요. locale 컬럼 값이 `null`이면 소명 프로세스가 정상 동작하지 않습니다.

**임직원 언어 설정**

언어는 한국어, 영어, 중국어 중에서 선택할 수 있습니다.

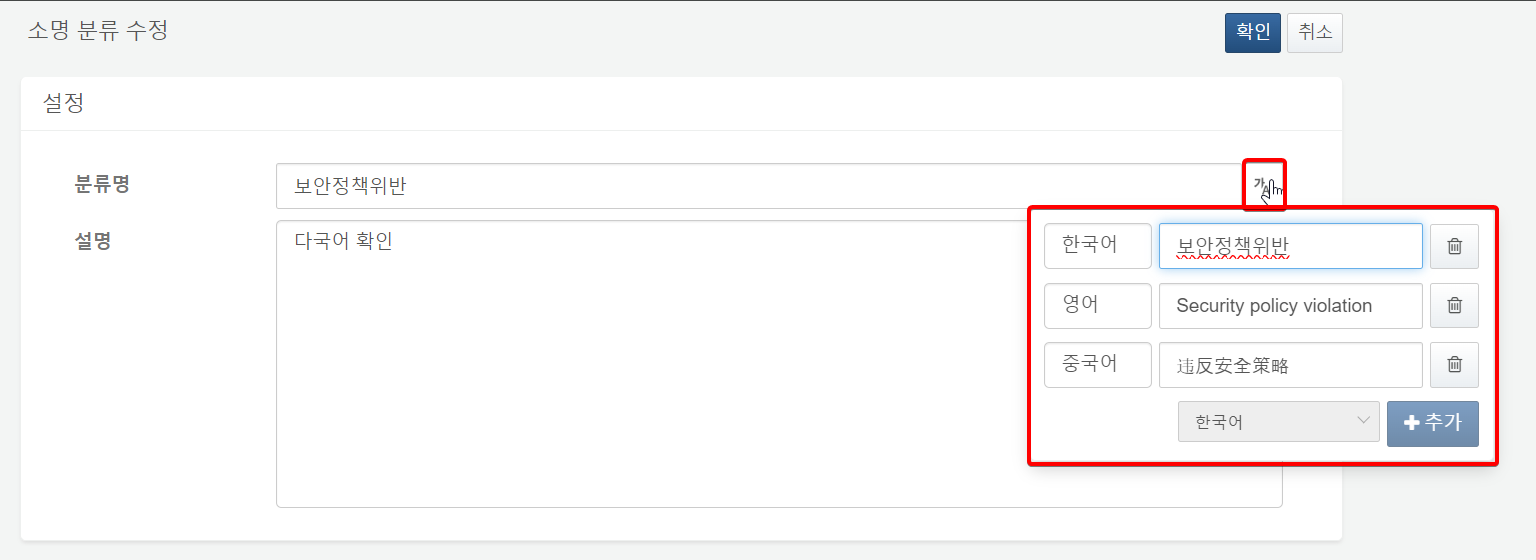


임직원의 언어 설정에 따라 소명 화면의 언어가 다르게 표시됩니다. 언어를 중국어로 설정한 경우 다음과 같이 표시됩니다.



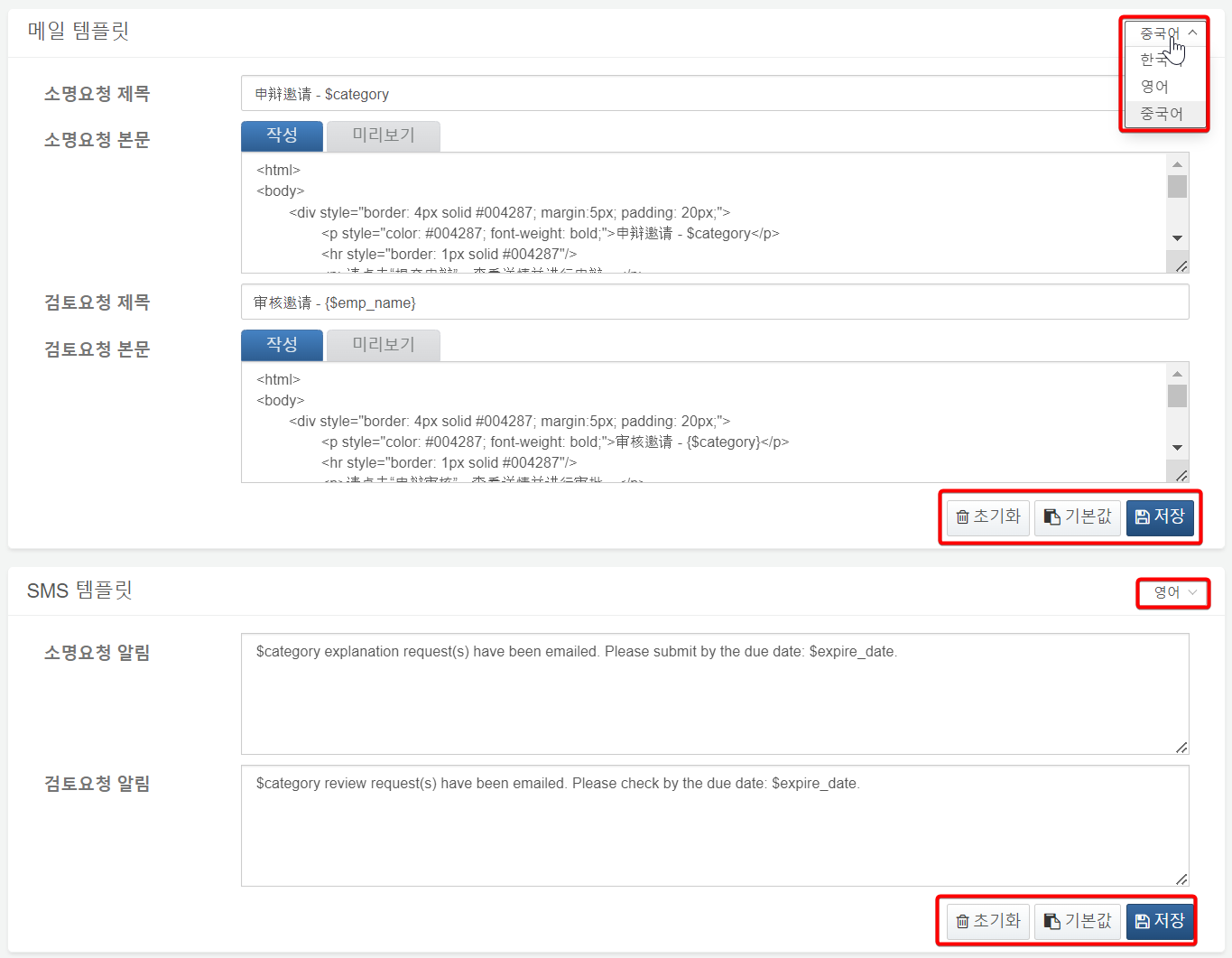
**소명 분류의 국제화**

소명 분류 설정 화면에서 분류명을 언어별로 지정할 수 있습니다.



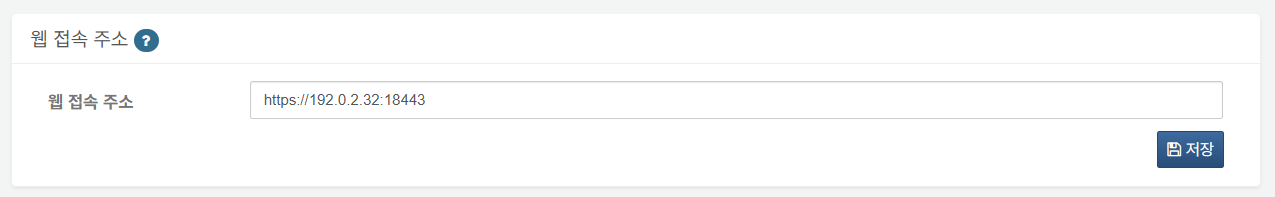
**소명 템플릿의 국제화**

소명 템플릿 화면에서 메일 템플릿과 SMS 템플릿을 언어별로 지정할 수 있습니다.



**소명 작성/검토 통신 포트 변경**

소명 요청 조회 및 검토 전용 통신에 TCP 18443 포트를 사용할 수 있도록 변경되었습니다. 소명 템플릿 화면에서 **웹 접속 주소**에 https://HOST:18443 형식으로 입력하면 TCP 18443 포트를 사용할 수 있습니다.

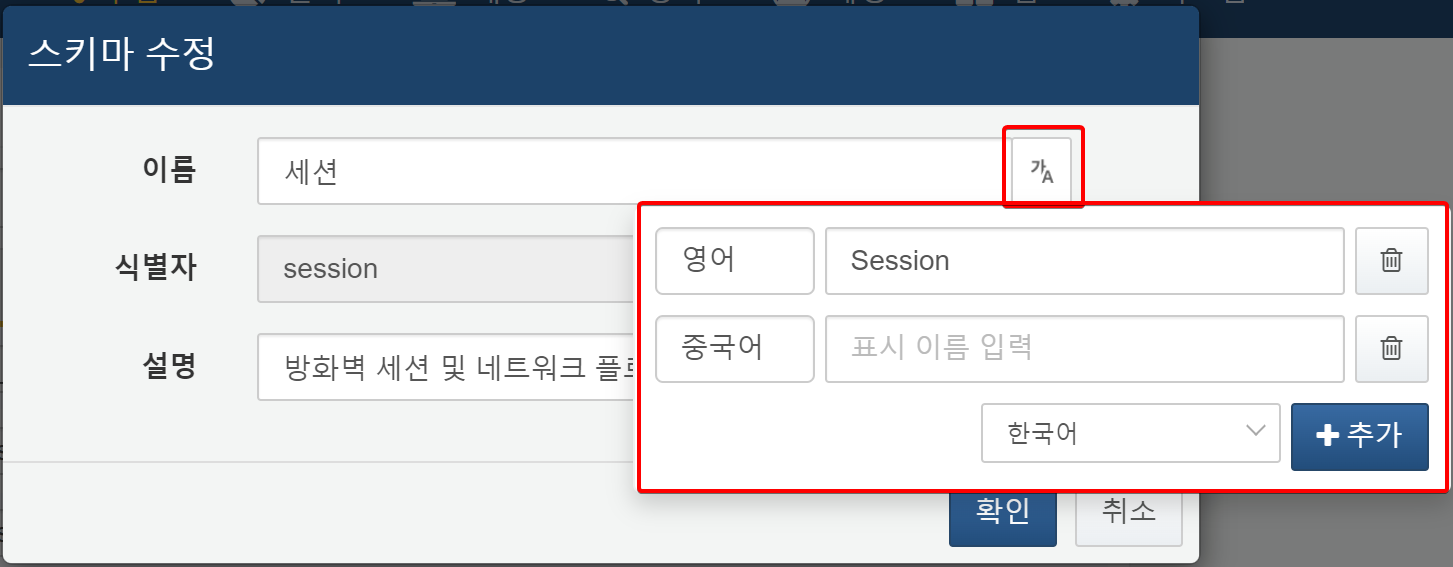


4.0.2404.0 버전으로 업그레이드 후 웹 접속 주소를 변경하지 않으면 이전에 설정한 웹 접속 주소와 포트를 그대로 이용하므로 별도의 조치를 하지 않아도 됩니다. 그러나 장기적으로 보안 관리 측면에서 두 통신을 분리하는 것이 바람직하므로 웹 콘솔 포트와 소명 포트를 나누어 사용하도록 권장합니다.

**로그 스키마의 국제화**

로그 스키마 다국어 지원이 추가되었습니다. 로그 스키마의 **이름**, 필드의 **표시 이름**을 각 언어에 따라 설정할 수 있습니다.각 항목 우측에 있는 다국어 버튼을 사용할 수 있고, 필드 표시 이름의 경우 언어 드롭다운 메뉴에서 특정 언어 선택 후 일괄 입력 가능합니다.

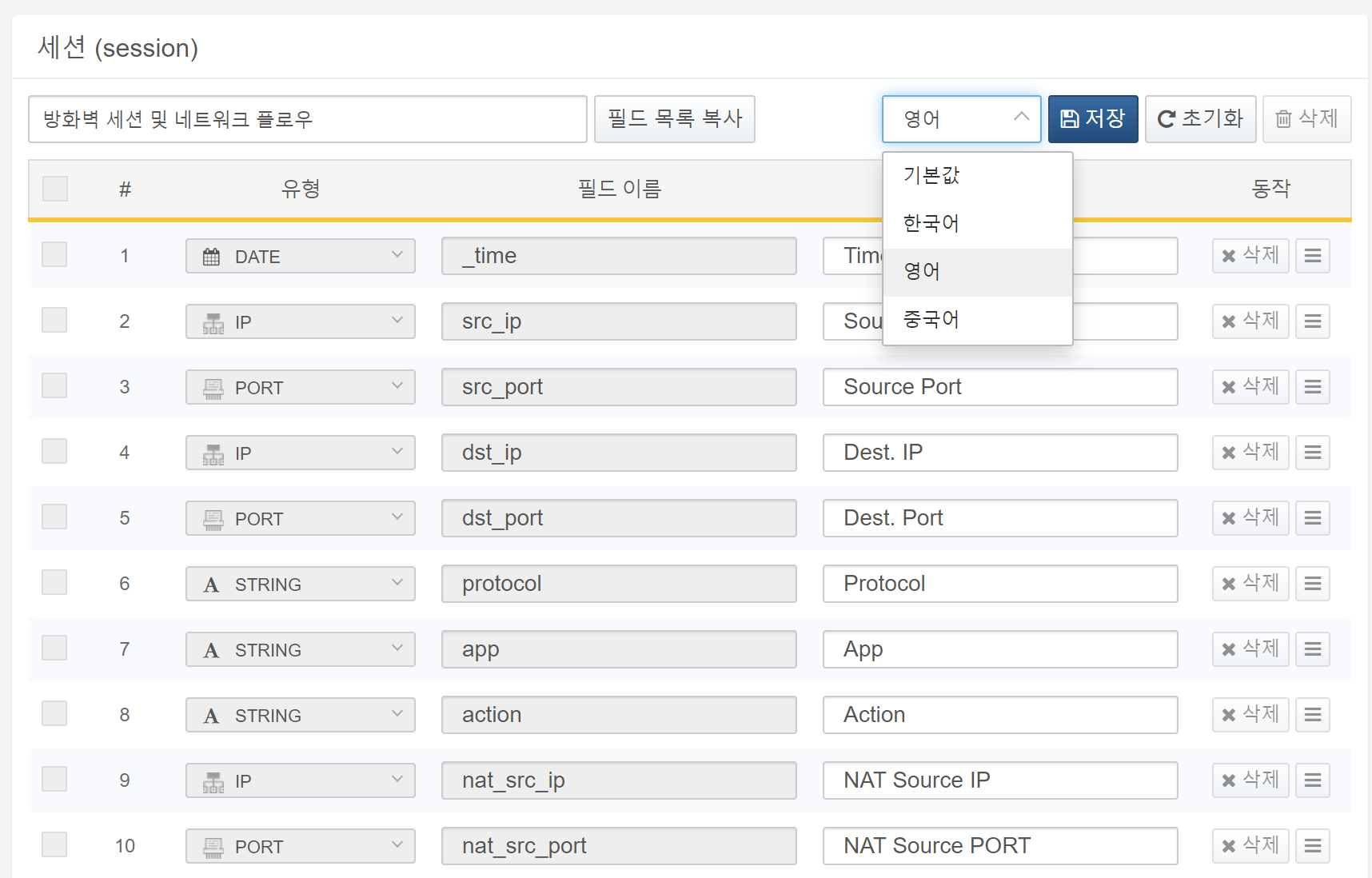
그 스키마의 이름을 다른 언어로 지정하려면 이름 우측에 있는 언어 버튼을 클릭하고 변경하세요.



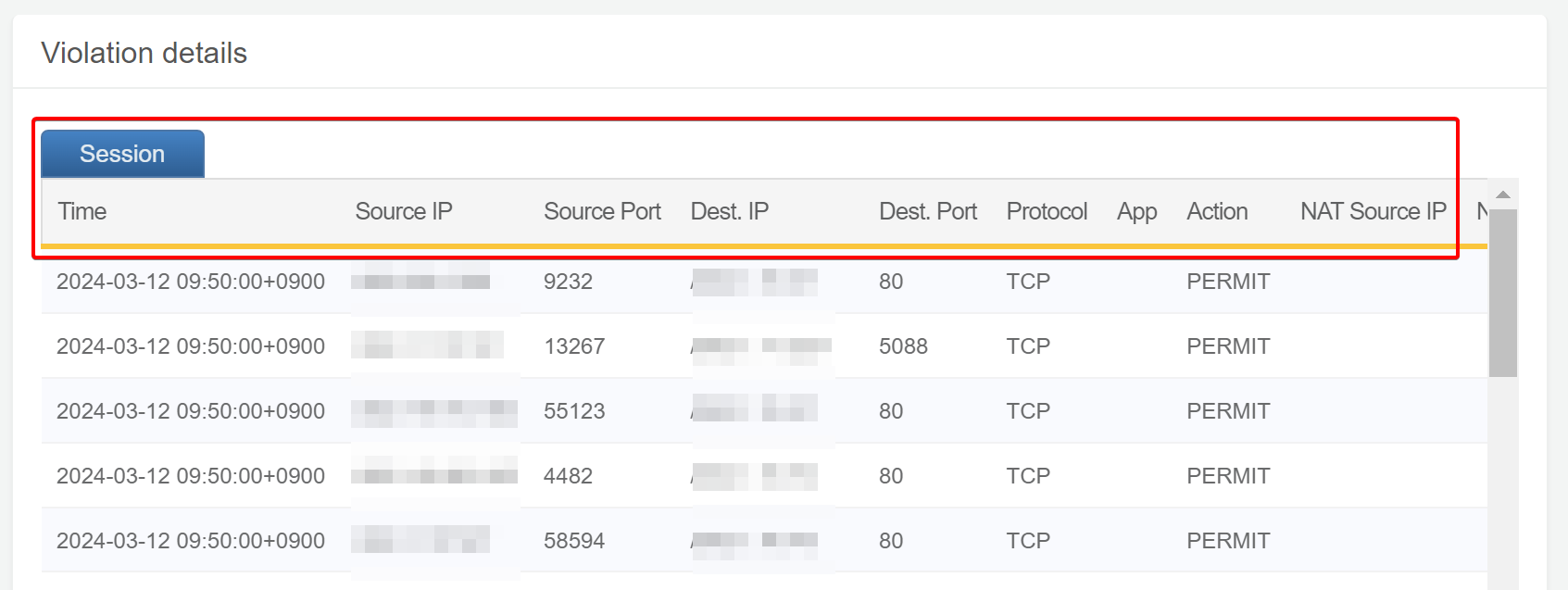
로그 스키마 필드의 표시 이름을 다른 언어로 지정하려면 표시 이름 우측에 있는 언어 버튼을 클릭하고 변경하세요.



로그 스키마를 다른 언어로 보려면 도구 모음에서 언어를 변경하세요.

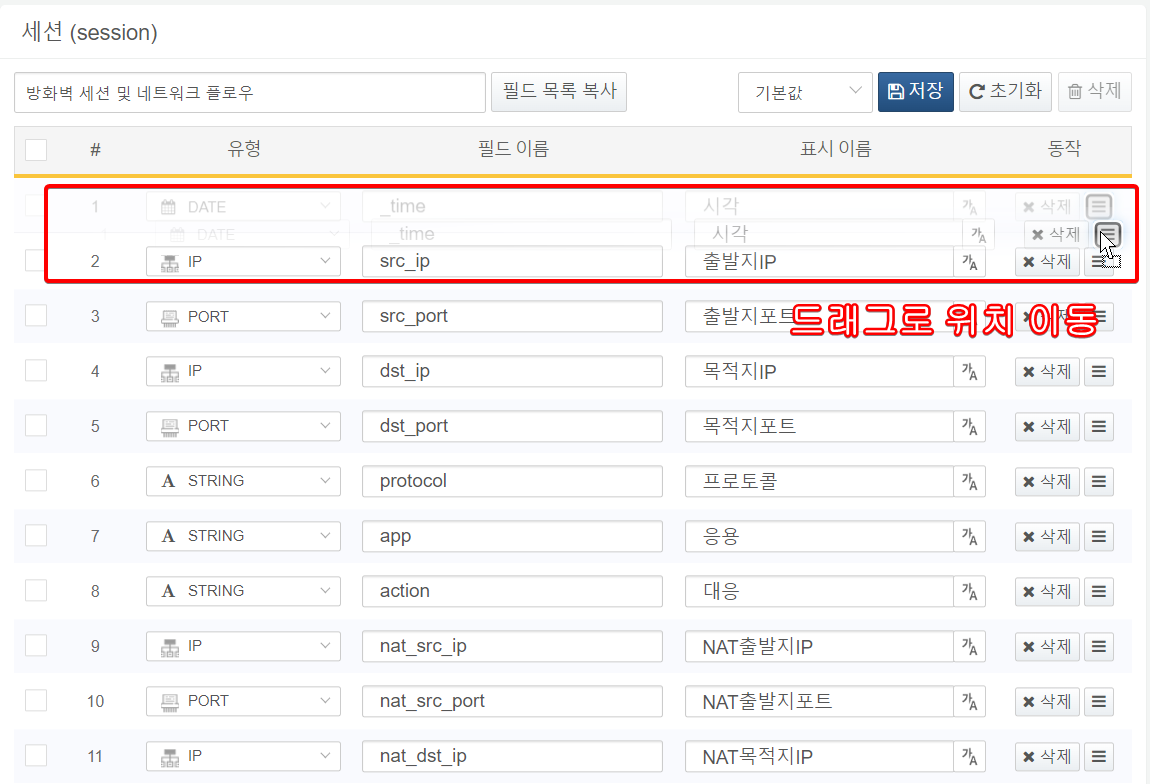


소명 화면 등에서 로그 스키마 표시할 때 다국어 설정이 적용됩니다.



**로그 스키마 필드의 순서 변경 개선**

필드의 순서를 쉽게 변경할 수 있도록 개선했있습니다. 필드 우측 핸들을 클릭한 다음 원하는 위치에 드래그해 놓으세요.

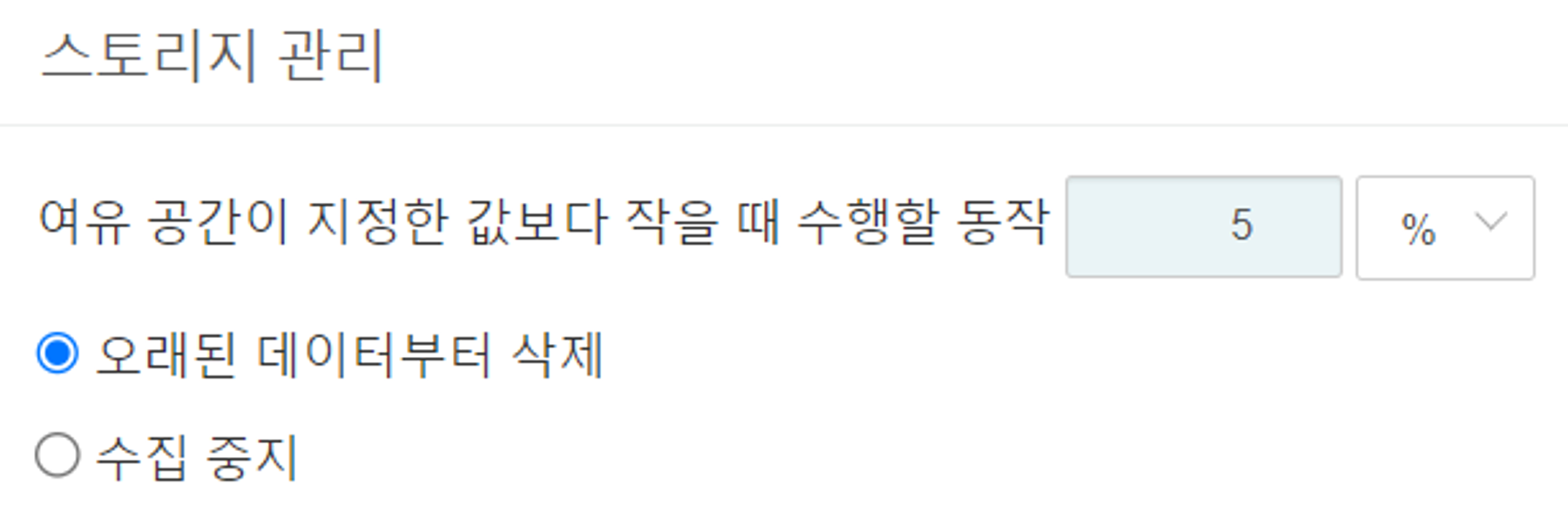


#### SNR#2291 OTP 기반 2단계 인증 지원

2단계 인증 수단으로 OTP를 지원합니다. 계정 설정에서 OTP 로그인 설정 시 계정 암호로 로그인 후 2차로 OTP를 입력해야만 로그인할 수 있습니다. 2단계 인증을 설정하는 방법은 [계정](https://docs.logpresso.com/ko/sonar/4.0/releases/ko/sonar/4.0/ui/section-users), 2단계 인증을 이용한 로그인은 [시작하기 - OTP 설정 및 인증](https://docs.logpresso.com/ko/sonar/4.0/releases/ko/sonar/4.0/ui/chapter-getting-started)을 참고하세요.

#### SNR#1541 디스크 고갈 대응 설정 추가

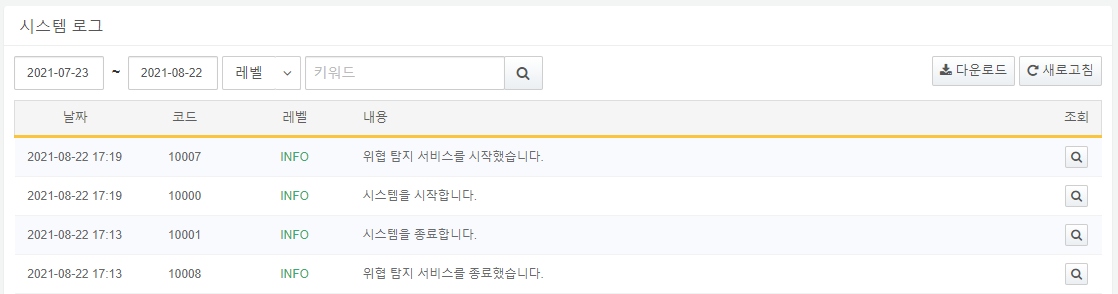
클러스터 노드의 스토리지 관리 기능이 추가되었습니다. 디스크 사용량이 임계치를 초과할 때 오래된 데이터부터 삭제하거나 데이터 수집을 중단하게 하도록 선택할 수 있습니다. 임계치는 디스크 잔여 비율(기본값 5%)이나 용량(기본값 100MB) 중 하나로 설정할 수 있고, 1분마다 디스크 고갈 여부를 확인해 디스크 고갈 상태가 해소되면 대응 작업을 중지합니다.



#### SNR#1542 시스템 로그 메뉴 추가

시스템 로그 조회 기능을 추가했습니다. 시스템 로그는 araqne.log 파일에서 확인 가능하지만 감사 로그 화면에서 표시되지 않던 시스템 로그를 표시합니다. 시스템 로그에 표시되는 정보는 다음 목록을 참고하세요.

* 시스템 종료 로그
* NTP 동기화 로그
* 저장 매체 임계치 로그
* 모든 항목에 대한 설정 변경 로그
* 사용자 로그인 실패 로그
* 무결성 검사 로그
* 상호 인증 로그



#### SNR#2097 percentile(), median() 추가

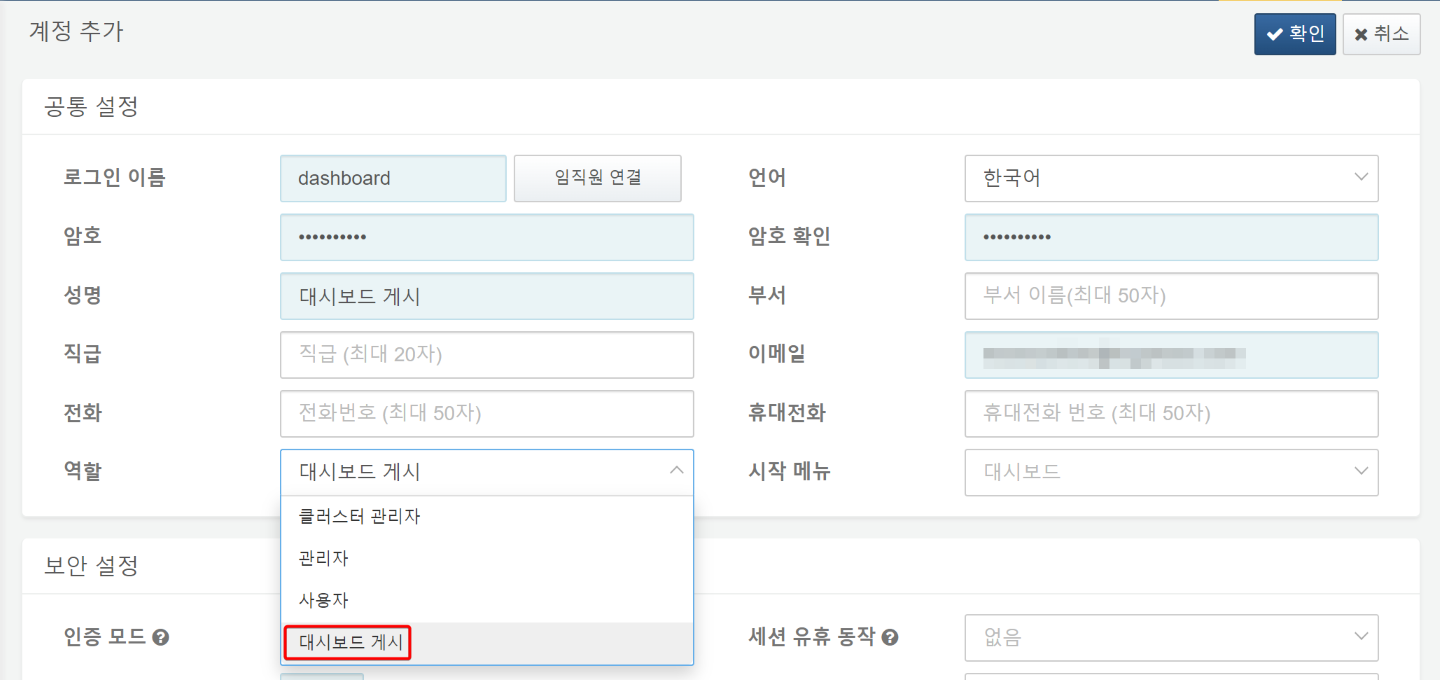
[percentile()](https://docs.logpresso.com/ko/sonar/4.0/releases/ko/query/percentile-aggregate-function), [median()](https://docs.logpresso.com/ko/sonar/4.0/releases/ko/query/median-aggregate-function)이 추가되었습니다.

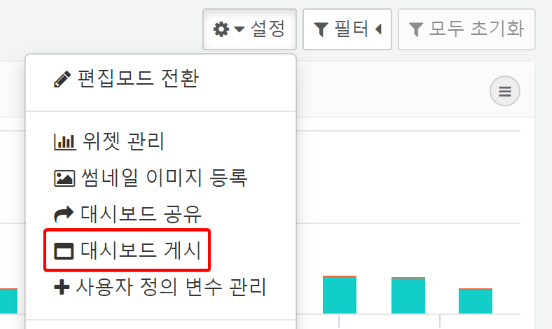
* percentile() 함수는 전체 데이터 중 특정 분위에 해당하는 값을 구하는 함수입니다. 백분위 기준으로 분위 값을 입력하며, 100은 최상위, 0은 최하위를 의미합니다.
* median() 함수는 전체 데이터 중 중간값을 구하는 집계 함수로, percentile(x,50,[interpolation])과 동일한 의미를 가집니다.
* percentile(x,0.0) 결과값은 min(x)와 동일하고 percentile(x,100.0) 결과값은 max(x)와 동일합니다.

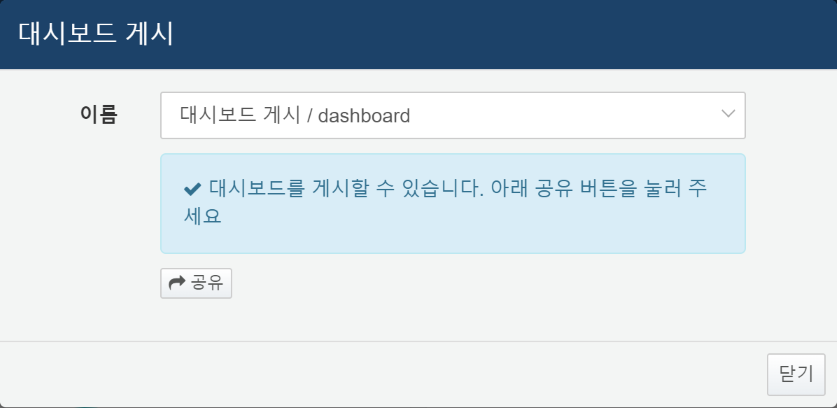
#### SNR#2143 대시보드 외부 게시 기능 및 대시보드 게시 전용 계정 유형 추가

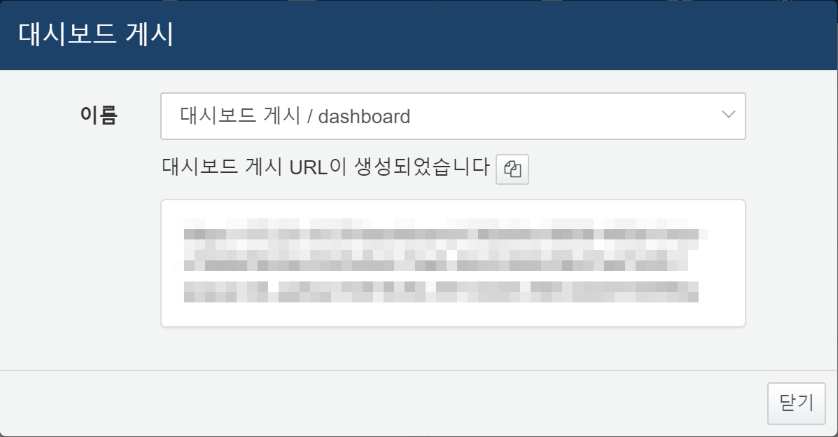
로그프레소 소나의 대시보드를 외부에 공유하는 기능을 추가했습니다.

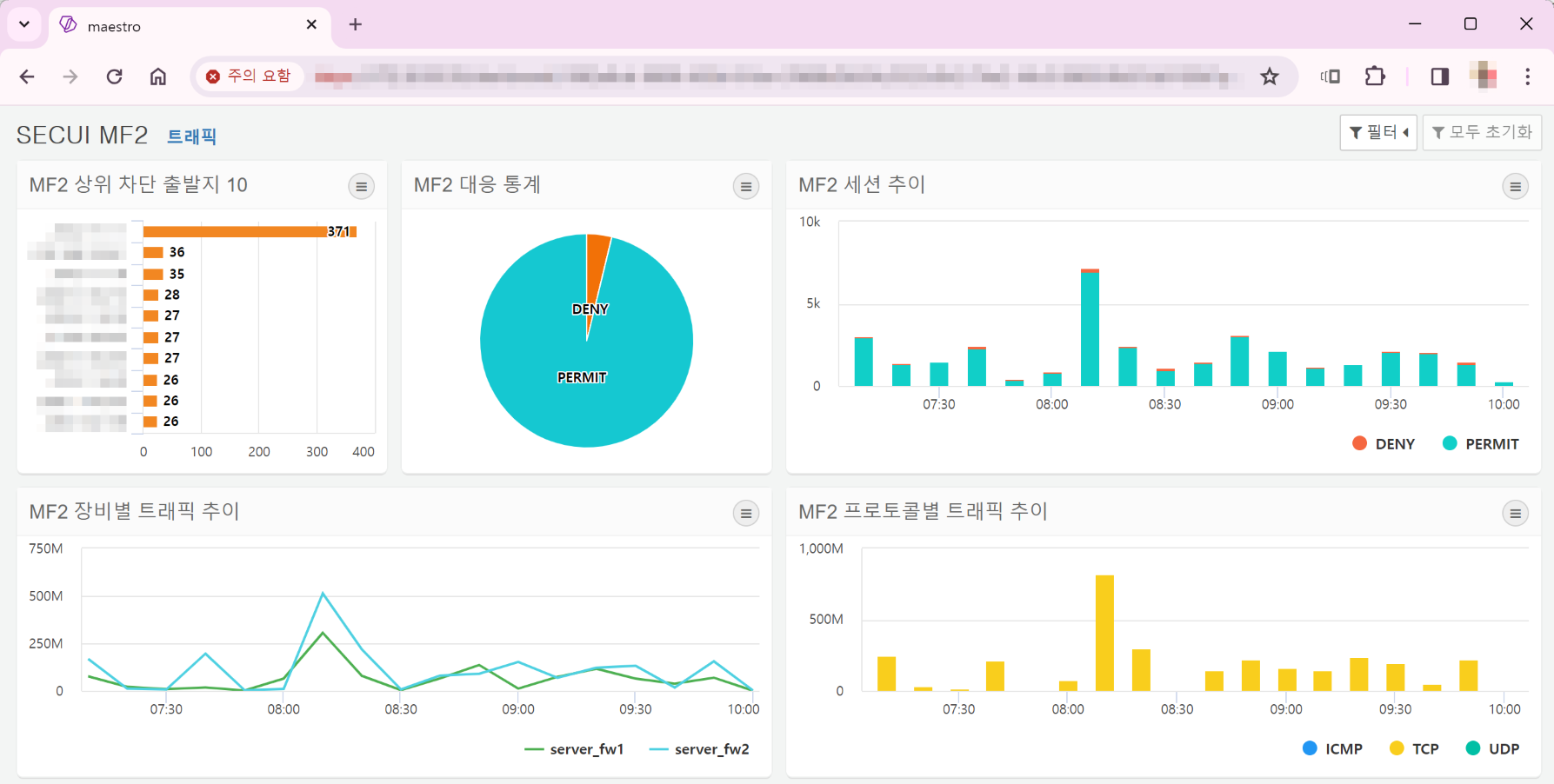
대시보드 공유를 하려면 대시보드 게시 유형 계정이 필요합니다. 다음과 같이 대시보드 게시 계정을 만들고 대시보드를 공유할 수 있습니다.

[계정](https://docs.logpresso.com/ko/sonar/4.0/releases/ko/sonar/4.0/ui/section-users) 화면에서 "대시보드 게시" 권한을 가진 계정을 생성하세요. 계정 생성 시 자동으로 API 키가 발급됩니다.

[대시보드](https://docs.logpresso.com/ko/sonar/4.0/releases/ko/sonar/4.0/ui/dashboard-settings) 화면에서 **대시보드 게시**를 클릭합니다.

대시보드 게시 대화상자에서 대시보드 게시 권한 계정을 선택하고 공유 버튼을 클릭하세요.

대시보드 공유 URL이 생성되면 클립보드에 URL을 복사하고 **닫기**를 클릭해 창을 닫으세요.

발급받은 대시보드 공유 URL을 필요한 곳에서 사용합니다.

#### SNR#2178 쿼리 자동완성 단축키 추가

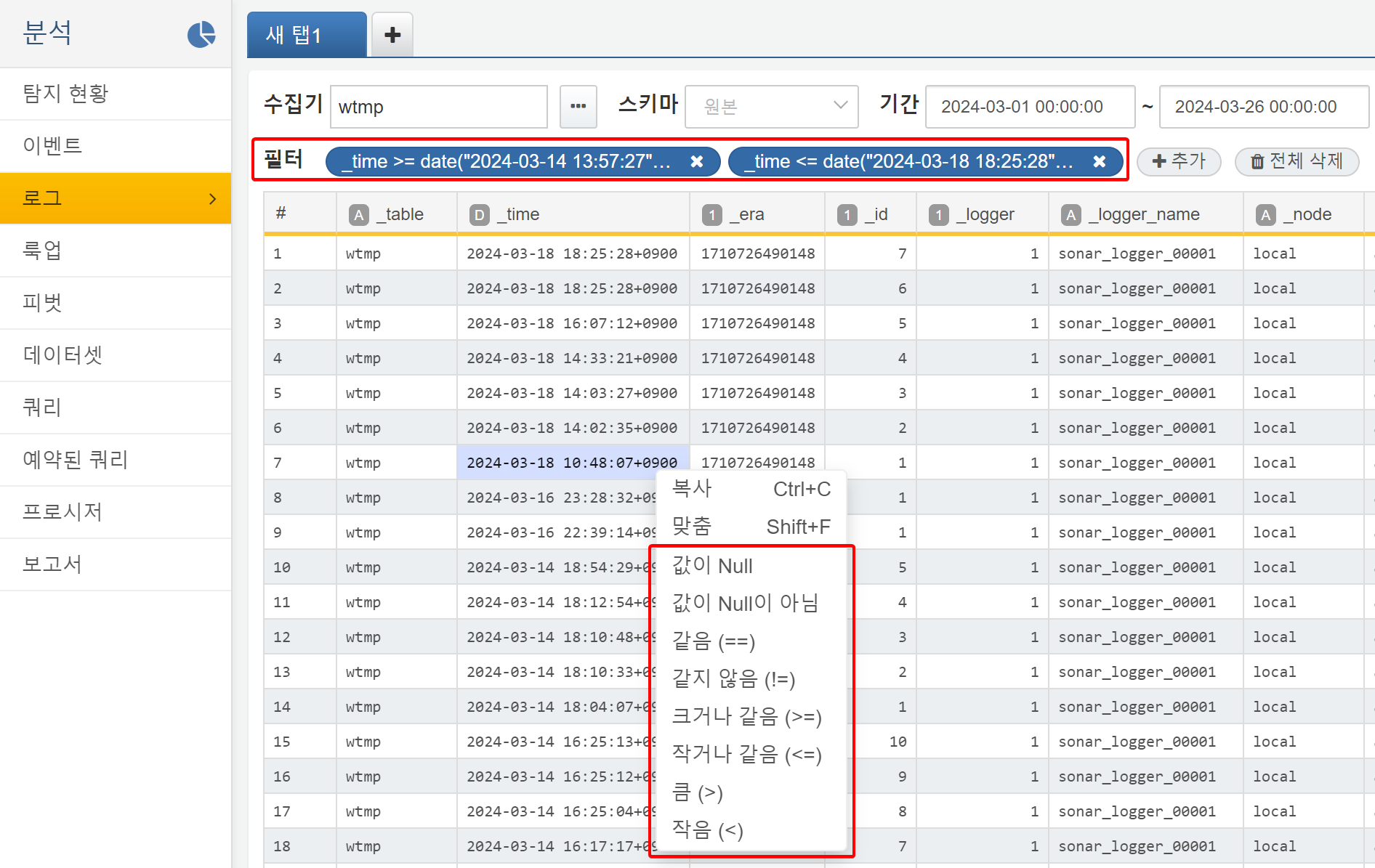
기존 쿼리 자동완성 단축키인 **Ctrl + Space**를 사용하기 어려운 상황이 존재하여, 쿼리 자동완성 단축키를 추가했습니다.

|  |  |
| --- | --- |
| 운영체제 | 단축키 |
| 윈도우 | **Ctrl + Space** 또는 **Ctrl + Shift + Space** |
| 맥 | **Ctrl + Space** 또는 **Command + Space** |

맥에서는 Command + Space 조합이 스팟라이트(Spotlight)의 단축키와 겹칠 수 있습니다.

#### SNR#2233 로그 화면의 날짜/시간 필터 개선

[로그](https://docs.logpresso.com/ko/sonar/4.0/releases/ko/sonar/4.0/ui/section-logs) 화면에서 날짜/시간 필터를 개선했습니다. 날짜 값에 오른쪽 클릭 시 표시되는 팝업 메뉴에 일치 및 비교 필터가 추가되었습니다.



#### SNR#2254 수집기 REST API 지원

수집기 REST API가 추가되었습니다.

* [수집기 목록 조회](https://docs.logpresso.com/ko/sonar/4.0/releases/ko/sonar/4.0/api/get-loggers)
* [수집기 조회](https://docs.logpresso.com/ko/sonar/4.0/releases/ko/sonar/4.0/api/get-logger)
* [수집기 생성](https://docs.logpresso.com/ko/sonar/4.0/releases/ko/sonar/4.0/api/create-logger)
* [수집기 수정](https://docs.logpresso.com/ko/sonar/4.0/releases/ko/sonar/4.0/api/update-logger)
* [수집기 일괄 삭제](https://docs.logpresso.com/ko/sonar/4.0/releases/ko/sonar/4.0/api/remove-loggers)
* [수집기 활성화](https://docs.logpresso.com/ko/sonar/4.0/releases/ko/sonar/4.0/api/enable-logger)
* [수집기 비활성화](https://docs.logpresso.com/ko/sonar/4.0/releases/ko/sonar/4.0/api/disable-logger)
* [수집기 상태 일괄 초기화](https://docs.logpresso.com/ko/sonar/4.0/releases/ko/sonar/4.0/api/reset-loggers)

#### SNR#2255 프로시저 REST API 지원

프로시저 REST API가 추가되었습니다

* [프로시저 목록 조회](https://docs.logpresso.com/ko/sonar/4.0/releases/ko/sonar/4.0/api/get-procedures)
* [프로시저 조회](https://docs.logpresso.com/ko/sonar/4.0/releases/ko/sonar/4.0/api/get-procedure)
* [프로시저 생성](https://docs.logpresso.com/ko/sonar/4.0/releases/ko/sonar/4.0/api/create-procedure)
* [프로시저 수정](https://docs.logpresso.com/ko/sonar/4.0/releases/ko/sonar/4.0/api/update-procedure)
* [프로시저 일괄 삭제](https://docs.logpresso.com/ko/sonar/4.0/releases/ko/sonar/4.0/api/remove-procedures)

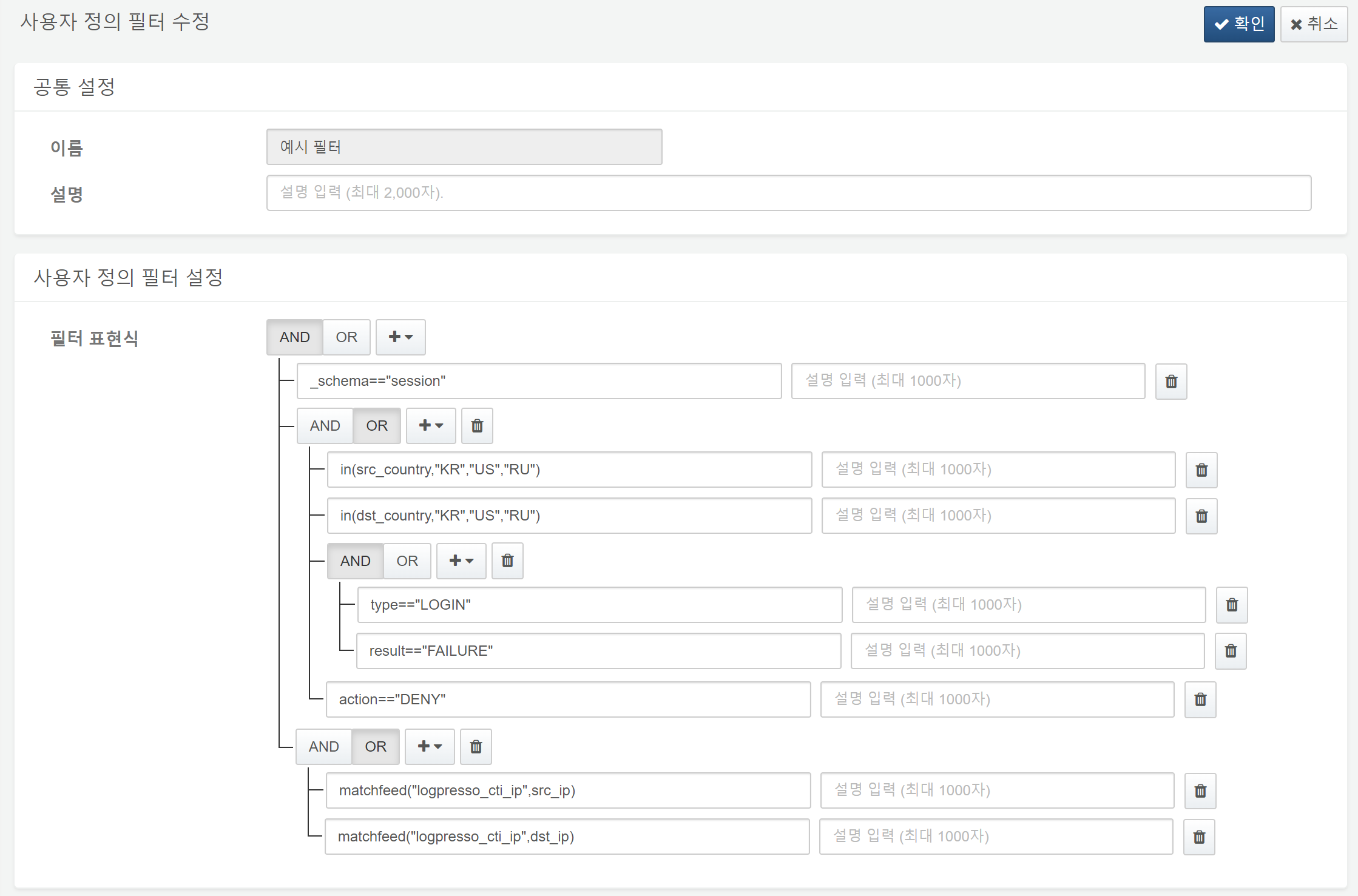
#### SNR#2280 parsejson 쿼리 명령어에 flatten, cutoff, lenient 옵션 추가

parsejson 쿼리 명령어가 더 다양하고 복잡한 형태의 JSON 데이터를 처리할 수 있도록 flatten, cutoff, lenient 옵션을 추가했습니다. 각 옵션에 대한 상세 내용은 [parsejson](https://docs.logpresso.com/ko/sonar/4.0/releases/ko/query/parsejson-command) 설명서를 참고하세요.

#### SNR#2281 사용자 정의 필터 화면에 AND/OR 그룹 트리 UI 추가

사용자 정의 필터를 설정할 때 AND/OR 구문으로 필터 그룹을 트리 형태로 구성할 수 있는 UI를 추가했습니다. AND/OR는 언제든 변경할 수 있습니다.

* AND/OR 그룹은 최상단 그룹을 포함하여 최대 4단계까지 만들 수 있습니다.
* 각 필터 표현식의 최대 길이는 1,000자입니다.

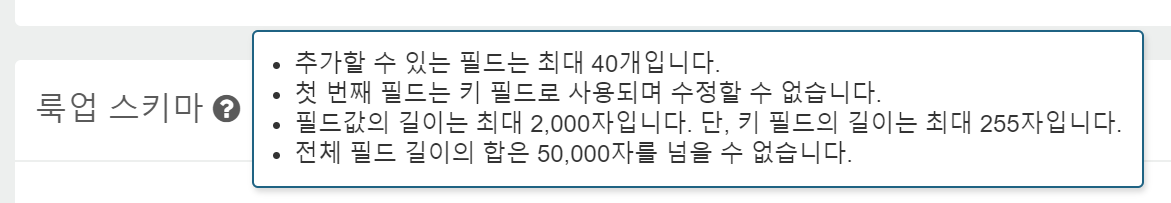


#### SNR#2287 보고서 메일 전송 쿼리 명령어 sonar-send-report 추가

sonar-send-report 쿼리 명령어가 추가되었습니다. sonar-export-report 명령어처럼 보고서를 생성해 내보낼 수 있고, 보고서를 메일로 전송하는 데에 사용됩니다. 상세 내용은 [sonar-send-report](https://docs.logpresso.com/ko/sonar/4.0/releases/ko/query/sonar-send-report-command) 설명서를 참고하세요.

#### SNR#2307 룩업 스키마 필드 길이 제약 완화

최대 필드 개수 10개, 필드 값의 최대 길이 255자로 제한되었던 룩업 스키마의 제약을 완화하였습니다. 필드는 최대 40개, 각 필드값의 최대 길이는 2,000자, 전체 필드 길이 제한은 50,000자로 변경했습니다.



#### SNR#2309 시스로그 TCP 전송 쿼리 명령어 sendsyslog-tcp 추가

시스로그 메시지를 TCP 통신으로 전송하는 쿼리 명령어 [sendsyslog-tcp](https://docs.logpresso.com/ko/sonar/4.0/releases/ko/query/sendsyslog-tcp-command)가 추가되었습니다.

[system-syslog-tcp-senders](https://docs.logpresso.com/ko/sonar/4.0/releases/ko/query/system-syslog-tcp-senders-command) 명령으로 sendsyslog-tcp명령에 따라 메시지를 전송하는 시스로그 전송기에 대한 진단 정보를 확인할 수 있습니다.

#### SNR#2432 system logs 쿼리 명령어에 tail 옵션 추가

[system logs](https://docs.logpresso.com/ko/sonar/4.0/releases/ko/query/system-logs-command) 쿼리 명령어에 tail 옵션이 추가되었습니다.

#### SNR#2172 인덱스 토큰 최대 길이를 255자로 제한

메일 본문에 포함된 BASE64 이미지 등 지나치게 긴 토큰을 인덱싱할 때 발생할 수 있는 성능 문제를 예방하기 위해 토큰 최대 길이를 255자로 제한하도록 변경했습니다. 토큰 최대 길이를 변경하려면 logpresso.index.max\_token\_len 시스템 스위치를 사용하세요.

# 토큰 최대 길이를 300으로 변경-Dlogpresso.index.max\_token\_len=300

#### SNR#2265 패턴 그룹에 패턴 대량 등록 시 시스템 부하가 발생하는 문제 해결

REST API 등을 사용하여 패턴 그룹에 1만 개 이상의 패턴을 한꺼번에 추가하면 패턴 개수만큼 패턴 그룹을 수정하면서 시스템 부하가 발생하는 문제가 있었습니다. 대량의 패턴 등록을 한 번에 처리하도록 개선했습니다.

#### SNR#2293 TCP 시스로그 서버에서 수신 오류 시 파일 누수가 발생하는 문제 해결

TCP 시스로그 세션 생성 후 일정 기간 동안 로그 수신이 없는 경우 세션 타임아웃을 하는 기능을 추가했습니다. 기본값은 60초(60,000ms)이고, logpresso.syslog.idle\_timeout 시스템 스위치로 값을 조정할 수 있습니다.

# TCP 시스로그 서버 세션 idle 타임아웃을 2분(120초)로 수정-Dlogpresso.syslog.idle\_timeout=120000

#### SNR#2344 특정 조건에서 행위 프로파일 동기화가 지연되는 문제 해결

다음 조건에서 분석B 서버에서 행위 프로파일 동기화가 최대 1분까지 지연되는 문제를 해결했습니다.

* 수집 노드가 로드밸런서를 통해 분석 노드에 부하 분산하여 접속하는 경우
* 분석 노드에서 정책 동기화 대상 주소를 127.0.0.1로 지정한 경우 (sonar.setMaster)

#### SNR#2367 TCP 시스로그 서버에서 파일 누수가 발생하는 문제 해결

TCP 시스로그 서버에서 시스로그 메시지를 수신하거나 읽다가 오류가 발생하면 파일 누수가 발생하는 문제를 해결했습니다.

#### SNR#2375 TCP 443 포트에 웹 콘솔 바인딩 실패 시 재시도 포트 번호를 4443으로 변경

4.0.2312.0 버전에서 로그프레소 엔터프라이즈 웹 콘솔이 8443 포트를 사용하도록 변경되면서 로그프레소 소나 웹 콘솔이 8443 포트를 사용할 수 없는 문제가 발생하였습니다. 로그프레소 소나 웹 콘솔이 TCP 443 포트를 사용할 수 없는 경우에는 4443 포트를 사용하도록 변경하여 포트 할당 문제를 해결했습니다.

#### SNR#2379 동일 일자 시스템 로그 파일을 두 번째 순환할 때 부팅이 불가능한 문제 해결

로그프레소 소나는 구동 시 시스템 로그 파일(araqne.log)을 1일 단위로 순환(Rotate)합니다. 예를 들어 시스템 시간이 2099년 1월 1일에서 1월 2일로 변경되면 araqne.log 파일의 이름을 araqne.log.2099-01-01로 변경하고, 새 araqne.log 파일을 생성합니다.

로그를 순환하는 시점에 araqne.log.2099-01-01 파일이 이미 있다면 araqne.log.2099-01-01을 araqne.log.2099-01-01.1로 이름을 변경하고, araqne.log 파일의 이름을 araqne.log.2099-01-01.2으로 변경한 후 새로운 araqne.log 파일을 생성해야 합니다. 그러나 araqne.log.yyyy-MM-dd.1 형식의 파일이 존재하는 경우 araqne.log.yyyy-MM-dd.2로 변경하지 못하고 작업을 무한히 반복하여 부팅이 불가능한 문제가 있어서 해결했습니다.

#### SNR#2383 분석 노드 설치 시 티켓 감사 로그 테이블의 이중화 설정 누락 해결

분석 서버에서 티켓 감사로그 테이블 (sonar\_ticket\_audit\_logs) 이중화 설정이 누락된 문제를 해결했습니다.

#### SNR#2385 테이블 백업, 복원 시 메모리 누수 문제 해결

테이블 데이터를 백업하거나 복원하는 과정에서 메모리 누수가 발생하는 문제를 해결했습니다. 영향받는 기능은 다음과 같습니다.

* [copytable](https://docs.logpresso.com/ko/query/copytable-command) 쿼리 명령어
* logstorage.backup, logpresso.restore 로그프레소 셸 명령어

#### SNR#2389 앱 재설치 시 앱 부속 모듈이 재설정되지 않던 문제 해결

앱 재설치 시 bundle.refresh 작업을 통한 번들 의존성 정리가 누락되어 앱이 제공하는 기능을 제대로 사용할 수 없던 문제를 해결했습니다.

#### SNR#2402 윈도우 서버 2016, 2012에서 센트리 자동 설치가 동작하지 않는 문제 해결

윈도우 서버 2016 R2, 2012 R2 등에서 파워셸 기본 설정이 TLS 1.2 버전을 지원하지 않을 때 센트리 자동 설치 스크립트가 제대로 수행되지 않는 버그가 있었습니다. 윈도우 센트리 자동 설치 스크립트가 윈도우 구 버전을 고려해 동작하도록 수정하여 해당 이슈를 해결했습니다.

#### SNR#2429 예약된 쿼리 실행 실패 시 오류 메시지가 255자를 초과하면 예약된 쿼리 상태가 변경되지 않는 문제 해결

예약된 쿼리의 실행 상태를 기록하는 sonar\_scheduled\_queries 테이블에서 실패 사유를 기록하는 컬럼은 255자의 제한이 있습니다. 예약된 쿼리 실행 실패 시 오류 메시지가 255자를 넘으면 예약된 쿼리 상태 변경 시도 시 SQL 오류가 발생해 상태를 변경할 수 없고, 예약된 쿼리를 중지하거나 비활성화하려고 해도 상태 변경이 되지 않으며 실행 상태에서 소요시간만 계속 증가하는 문제가 있었습니다. 예약된 쿼리 상태 변경 시 실패 사유 메시지를 255자로 잘라 저장함으로써 해당 문제를 해결했습니다.

오류 메시지가 255자를 초과해 예약된 쿼리 상태 변경에 실패하면 araqne.log 파일에서 다음과 같은 로그를 볼 수 있습니다.

[2024-03-19 10:11:15,364] WARN (DefaultQuery) - araqne logdb: query [1645] status callback should not throw any exceptionjava.lang.IllegalStateException: sonar sql [UPDATE sonar\_scheduled\_queries SET running\_state=?, result\_state=?, last\_failed\_at=?, fail\_reason=?, running\_time=? WHERE guid=?] 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.dom.impl.SqlConnectorImpl.\_\_M\_execute(SqlConnectorImpl.java:391) at com.logpresso.sonar.dom.impl.SqlConnectorImpl.execute(SqlConnectorImpl.java) ...Caused by: java.sql.SQLDataException: (conn=140) Data too long for column 'fail\_reason' at row 1 ...Caused by: java.sql.SQLException: Data too long for column 'fail\_reason' at row 1 ...

#### SNR#2436 CentOS 7 서버에서 센트리 자동 설치가 실패하는 문제 해결

CentOS 7 서버에서 센트리 자동 설치 스크립트 수행 시 적절한 버전의 JRE 패키지를 찾지 못해 설치가 실패하는 문제를 해결했습니다.

#### SNR#2440 인덱스 생성 시 블룸필터 활성화

테이블 생성 시 자동 생성되는 인덱스가 블룸필터를 사용하도록 수정했습니다.

#### SNR#2470 sonar-node 번들 재시작 시 소나 웹 콘솔 접속 등 일부 기능이 동작하지 않는 문제 해결

sonar-node 번들 재시작 시 sonar-core 등 일부 번들 재시작에 실패하여 웹 콘솔 등 일부 소나 기능이 동작하지 않던 문제를 해결했습니다.

#### SNR#2088 nvl 함수 호출 시 원본 필드 오염 문제 해결

[nvl()](https://docs.logpresso.com/ko/sonar/4.0/releases/ko/query/nvl-function) 함수에 값이 null인 필드를 매개변수로 전달하면, nvl 함수 실행 후 매개변수로 전달한 필드의 값이 의도하지 않게 DEFAULT\_EXPR 값으로 덮어씌워지는 문제를 해결했습니다.

#### SNR#2354 sonar-export-report 쿼리 명령어의 PDF 파일 생성 지원

[sonar-export-report](https://docs.logpresso.com/ko/sonar/4.0/releases/ko/query/sonar-export-report-command) 쿼리 명령어가 지원하는 보고서 파일 유형에 PDF를 추가했습니다.

#### SNR#2362 0 이하의 데이터에 대한 최댓값이나 양의 무한대 데이터에 대한 최솟값을 잘못 계산하는 문제 해결

[max()](https://docs.logpresso.com/ko/sonar/4.0/releases/ko/query/max-aggregate-function) 집계 함수가 숫자형 데이터에 대해 최댓값을 구할 때 최댓값이 0 이하인 경우 최댓값 대신 5e-324가 출력되는 문제를 해결했습니다.

[min()](https://docs.logpresso.com/ko/sonar/4.0/releases/ko/query/min-aggregate-function) 집계 함수가 양의 무한대(+Infinity)값만 존재하는 데이터의 최솟값을 구하는 경우 양의 무한대 대신 1.7976931348623157E308가 출력되는 문제를 해결했습니다.

#### SNR#2363 특정한 상황에서 sort, stats 쿼리 명령문이 by로 끝나는 필드명을 잘못 파싱하는 문제 해결

[sort](https://docs.logpresso.com/ko/sonar/4.0/releases/ko/query/sort-command), [stats](https://docs.logpresso.com/ko/sonar/4.0/releases/ko/query/stats-command) 등 by 절을 사용할 수 있는 쿼리 명령어에서 by 절을 사용하지 않고, 명령어 구문이 by로 끝나는 필드명일 경우 쿼리 명령어 파싱이 잘못되는 문제를 해결했습니다. 문제가 된 상황은 다음과 같습니다.

* sort standby -> sort stand by 로 파싱
* stats count as standby → stats count as stand by 로 파싱
* sort standby, action → 정상 파싱
* sort standby by bigsby → 정상 파싱
* stats count by bigsby → 정상 파싱

#### SNR#2378 쿼리 ID가 2,147,483,647를 초과하는 경우 쿼리 파싱에 실패하는 문제 해결

쿼리 실행 시 부여되는 쿼리 ID가 32비트 정수 최댓값(2,147,483,647)을 초과하는 경우 쿼리 파싱에 실패하여 쿼리가 실행되지 않고 cannot parse [$result$-2310877698] 오류 로그가 발생했습니다. 쿼리 ID가 32비트 정수 최댓값에 도달하면 다시 1번부터 시작하도록 수정했습니다.

#### SNR#2400 result 쿼리 명령어 성능 복원

4.0.2312.0 버전에서 [result](https://docs.logpresso.com/ko/sonar/4.0/releases/ko/query/result-command) 쿼리 명령어에 벡터화가 적용되지 않아 성능이 저하되는 문제를 해결했습니다.

#### SNR#2409 특정 테이블을 대상으로 동시에 purge 쿼리문 실행 시 낮은 확률로 해당 테이블에 쓰기 잠금이 해제되지 않는 문제 해결

특정 테이블을 대상으로 여러 건의 [purge](https://docs.logpresso.com/ko/sonar/4.0/releases/ko/query/purge-command) 명령을 동시에 수행할 경우 간헐적으로 테이블 쓰기 잠금(write lock)이 풀리지 않아 해당 테이블에 데이터를 입력할 수 없게 되고, 테이블에 데이터를 넣으려는 센트리의 RPC 접속 재시도로 트래픽이 증가하면서 센트리 접속이 끊기는 문제를 해결했습니다.

#### SNR#2449 setq [dbquery] 형태의 쿼리가 실패하는 문제 해결

[setq](https://docs.logpresso.com/ko/sonar/4.0/releases/ko/query/setq-command) 쿼리 명령어의 서브쿼리에 [dbquery](https://docs.logpresso.com/ko/sonar/4.0/releases/ko/query/dbquery-command) 쿼리 명령어를 사용하면 쿼리가 실패하는 문제를 해결했습니다. 이 문제는 4.0.2312.0 버전부터 발생했으며 이번 패치로 해결됐습니다.

이러한 문제가 발생했을 때 araqne.log 파일에서 확인할 수 있는 로그는 다음과 같습니다.

[2024-03-29 11:39:23,629] ERROR (QueryTaskRunner) - araqne logdb: query [7325] task [query: 7325 scan: dbquery sonar select 1] failedjava.lang.IllegalStateException: dbquery failed: select 1, Operation not permit on a closed resultSet at org.logpresso.jdbc.impl.DbQueryCommand.run(DbQueryCommand.java:119) ...Caused by: java.sql.SQLException: Operation not permit on a closed resultSet ...

#### SNR#2453 분산 쿼리 시 쿼리 종료와 쿼리 결과 처리 스레드가 확률적으로 경쟁하며 메모리가 누수되는 문제 해결

분산 쿼리 시 확률적으로 쿼리 종료와 쿼리 결과 처리 스레드가 경쟁하여 웹소켓이 무한 대기 상태에 빠지면서 누수되어 메모리 점유가 증가하면서 성능 저하 및 시스템 장애가 발생하는 문제를 해결했습니다.

#### SNR#2352 파이 차트 생성 시 "독립 변수와 종속 변수를 설정해야 합니다." 메시지가 출력되며 생성 실패하는 문제 해결

파이 차트 위젯 생성 시 독립 변수와 종속 변수를 설정해도 "독립 변수와 종속 변수를 설정해야 합니다." 메시지가 뜨며 위젯 생성이 실패하는 문제를 해결했습니다.

#### SNR#2472 파이 차트 클릭 이벤트에서 $필드이름$ 매크로 값이 잘못 매핑되는 문제 해결

파이 차트 클릭 이벤트 쿼리에 $필드이름$ 매크로를 설정한 경우, 실제 클릭 이벤트 발생 시 사용자가 클릭한 영역에 해당하는 필드 값이 제대로 나오지 않는 문제를 해결했습니다.

#### SNR#2167 수집기가 수천 개 이상일 때 수집기 목록 화면에 부하가 걸리는 문제 해결

수집기가 수천 개 이상일 때 수집기 전체 목록을 표시하는 화면이 매우 느려지는 문제를 해결했습니다. 이번 버전부터 수집기 목록은 전체를 표시하는 대신 상위 50건만 표시하며, 원하는 수집기가 50건 중에 없는 경우 수집기 이름을 검색해야 표시됩니다.

변경된 화면 목록은 다음과 같습니다.

* **분석 > 쿼리**: 수집기 선택
* **분석 > 데이터셋**: 수집기 데이터소스
* **분석 > 로그**: 수집기 선택
* **분석 > 피벗**: 수집기 선택
* **정책 > 실시간 시나리오 생성/편집**: 수집기 선택

#### SNR#2230 파서 목록 이동 시 기존 검색어 및 페이지 번호 유지

파서 생성 혹은 편집 후 파서 목록 화면으로 돌아갈 때 기존 검색어 및 페이지 번호를 유지하도록 수정했습니다. 이제 파서를 생성하거나 편집한 후 목록에서 다음 파서를 확인하기 위해 검색 및 페이지 이동을 처음부터 다시 수행하지 않아도 됩니다.

#### SNR#2251 수집기 편집 화면에서 값이 없는 항목에 대해 기본값을 표시하는 문제 해결

수집기 편집 화면에서 수집기 설정을 출력할 때 실제로 값이 없더라도 해당 항목의 기본값을 표시해서 마치 해당 항목에 값이 설정된 것처럼 보이는 문제를 해결했습니다. 패치 후 값이 없는 설정 항목은 기본값이 아니라 빈 문자열을 표시합니다.

#### SNR#2271 파서 설정에 입력 가능한 문자열 길이 제한 추가

파서 설정 입력 시 입력하는 문자열에 대한 길이 제한 등 유효성 검사가 추가되었습니다.

|  |  |  |  |
| --- | --- | --- | --- |
| 파서 유형 | 설정 항목 (영문) | 설정 항목 (한글) | 유효성 검사 |
| CEF | ver | 버전 | 최솟값 1, 최댓값 2 |
| CSV | use\_tab | 탭문자 사용 여부 | 허용값 true, false |
| CSV | use\_double\_quote | 큰 따옴표 이스케이프 | 허용값 true, false |
| CSV | column\_headers | 필드 이름 목록 | 허용 문자열 길이 0~10,000자 |
| CSV | target\_field | 대상 필드 | 허용 문자열 길이 0~255자 |
| CSV | include\_target | 원본 값 포함 여부 | 허용값 true, false |
| JSON | target\_field | 대상 필드 | 허용 문자열 길이 0~255자 |
| JSON | include\_target | 원본 값 포함 여부 | 허용값 true, false |
| 고정 길이 | column\_headers | 필드 이름 목록 | 허용 문자열 길이 0~10,000자 |
| 고정 길이 | column\_length | 필드 길이 목록 | 허용 문자열 길이 0~10,000자 |
| 고정 길이 | target\_field | 대상 필드 | 허용 문자열 길이 0~255자 |
| 고정 길이 | include\_target | 원본 값 포함 여부 | 허용값 true, false |
| 구분자 | delimiter\_target | 대상 필드 | 허용 문자열 길이 0~255자 |
| 구분자 | delimiter | 구분자 | 허용 문자열 길이 1~10자 |
| 구분자 | column\_headers | 필드 이름 목록 | 허용 문자열 길이 0~10,000자 |
| 구분자 | include\_delimiter\_target | 원본 값 포함 여부 | 허용값 true, false |
| 그루비 | script\_name | 스크립트 이름 | 허용 문자열 길이 1~255자 |
| 자바스크립트 | script\_name | 스크립트 이름 | 허용 문자열 길이 1~255자 |
| 정규표현식 | regex | 정규표현식 | 허용 문자열 길이 1~10,000자 |
| 정규표현식 | field | 대상 필드 | 허용 문자열 길이 0~255자 |
| 정규표현식 | include\_original\_field | 원본 필드 포함 | 허용값 true, false |
| 쿼리 | query | 쿼리 | 허용 문자열 길이 1~50,000자 |
| 태그 | tags | 태그 목록 | 허용 문자열 길이 1~10,000자 |
| 파서 선택기 | predicates | 파서 조건 선택식 | 허용 문자열 길이 1~1,000자, 조건 최대 1,000자, 파서 이름 최대 50자 |
| 파서 체인 | parsers | 파서 이름 목록 | 허용 문자열 길이 1~1,000자 |
| 필드 이름 변경 | mappings | 필드 이름 변환 목록 | 허용 문자열 길이 1~10,000자 |



#### SNR#2315 PCAP 디렉터리 와처 수집기가 payload 항목 수집을 누락하는 문제 해결

PCAP 디렉터리 와처 수집기로 pcap 파일 수집 시 payload 항목이 수집에서 누락되는 문제를 해결했습니다.

#### SNR#2325 SNMP 인터페이스 통계 수집기가 1개만 동작하는 문제 해결

SNMP 인터페이스 통계 수집기를 정상적으로 여러 개 만들어도 하나의 수집기만 값을 수집하는 문제를 해결했습니다.

#### SNR#2411 수집 모델에서 사용 중인 스키마 삭제 시도 시 오류 메시지를 명확하게 표시하도록 수정

수집 모델에서 사용 중인 로그 스키마를 삭제하려고 하면 오류 메시지를 "**다른 수집 모델에서 사용 중인 스키마입니다.**"로 명확히 표시하도록 수정했습니다.

#### SNR#1477 티켓 첨부 파일 삭제 불가 및 미리보기 깨짐 문제 해결, 크기 15MB 제한

티켓 추가 시 첨부 파일이 삭제되지 않는 문제, 이미지 파일이 아닌 첨부 파일 추가 시 깨진 미리보기 항목이 생기는 문제를 해결했습니다. 추가로 첨부 파일 최대 크기를 15MB로 제한하도록 수정했습니다.

#### SNR#2176 중복 티켓 축약 시 변경되지 않아야 할 값들이 수정되는 문제 해결

중복 티켓 축약 시 기존 출발지IP, 출발지포트, 목적지IP, 목적지포트, 프로토콜 등의 값이 나중에 발생한 티켓의 값으로 수정되어 외부 시스템에 전달된 기존 티켓 데이터로 해당 티켓을 검색할 수 없는 문제가 있었습니다. 패치 후 해당 값들을 업데이트하지 않도록 수정하여 문제를 해결했습니다.

배치 시나리오에서 생성된 티켓의 최근 발생 시각 값이 원본 이벤트의 시각 값이 아니라 배치 시나리오 실행 시간이 입력되던 문제를 해결했습니다.

#### SNR#2240 티켓 직접 생성 시 생성자가 시스템으로 잘못 표시되는 문제 해결

티켓 메뉴에서 티켓 직접 생성 시 생성자가 본인이 아닌 시스템으로 표시되는 문제가 해결됐습니다.

#### SNR#2313 반려된 티켓의 상태 변경이 불가능한 문제 해결

결재자가 반려한 티켓을 담당자가 다시 처리 중으로 변경하려고 할 때 상태가 변경되지 않는 문제를 해결했습니다.

#### SNR#2326 티켓이 대량 발생한 날짜 범위에 대해 태그 검색 시 성능이 저하되는 문제 해결

티켓이 많은 날짜 범위를 대상으로 태그 검색을 할 경우 1초 가량 걸리던 검색이 10초 대로 느려지는 문제가 있었습니다. SQL 쿼리문 최적화를 적용하여 티켓 태그 검색 성능을 개선했습니다.

#### SNR#2358 티켓 제목이 255자를 초과하면 티켓 생성이 실패하는 문제 해결

탐지 시나리오를 통해 티켓을 자동으로 생성할 때 티켓 제목이 255자를 초과하면 티켓을 생성하지 못하는 문제를 해결했습니다.

[2024-04-03 16:28:07.899] ERROR (StreamQuery) - logpresso query: stream query [sonar\_event] push failedjava.lang.IllegalStateException: cannot create ticket ea8a953e-202b-4cbb-a396-83a5596f1591, title=123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890 ${계정} ${계정} ${계정} at com.logpresso.sonar.api.impl.TicketServiceImpl.\_\_M\_createTicket(TicketServiceImpl.java:736) at com.logpresso.sonar.api.impl.TicketServiceImpl.createTicket(TicketServiceImpl.java) at com.logpresso.sonar.api.impl.AlertServiceImpl.\_\_M\_generateTicket(AlertServiceImpl.java:600) at com.logpresso.sonar.api.impl.AlertServiceImpl.generateTicket(AlertServiceImpl.java) ...Caused by: java.lang.IllegalStateException: sonar sql [INSERT INTO sonar\_tickets (repo\_id, guid, title, format, content, owner\_id, site\_id, stream\_rule\_id, status, priority) VALUES (?,?,?,?,?,?,?, 53,?,?)] failure at com.logpresso.sonar.dom.impl.SqlConnectorImpl.\_\_M\_execute(SqlConnectorImpl.java:268) at com.logpresso.sonar.dom.impl.SqlConnectorImpl.execute(SqlConnectorImpl.java) ...Caused by: java.sql.SQLDataException: (conn=23700) Data too long for column 'title' at row 1 ...Caused by: java.sql.SQLException: Data too long for column 'title' at row 1 ...

#### SNR#2433 티켓의 태스크 탭 조회 시 실행 중인 플레이북이 존재하는 경우 새로고침 주기마다 화면이 위로 이동하는 문제 해결

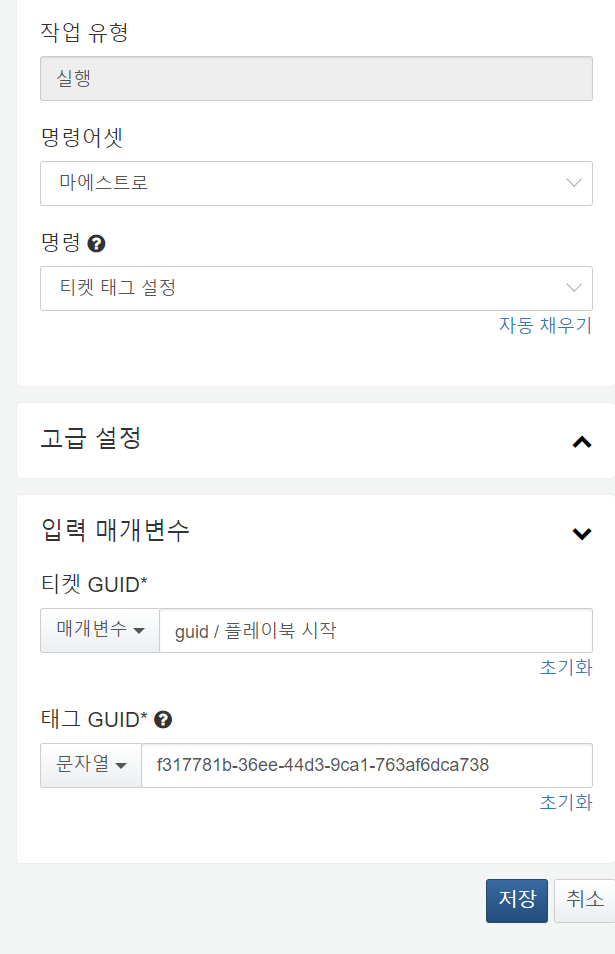
티켓의 태스크 탭에 실행 중인 플레이북이 존재하는 경우, 태스크 탭이 새로고침 주기에 도달할 때마다 스크롤이 초기화되면서 화면이 최상단으로 이동하는 문제가 있었습니다. 새로고침 주기에 도달해도 스크롤이 초기화되지 않도록 수정하여 문제를 해결했습니다.

#### SNR#2441 티켓 생성 REST API 호출 시 NullPointerException 예외 발생하며 실패하는 문제

티켓 생성 REST API 호출 시 NullPointerException 예외가 발생하며 실패하는 문제를 해결했습니다.

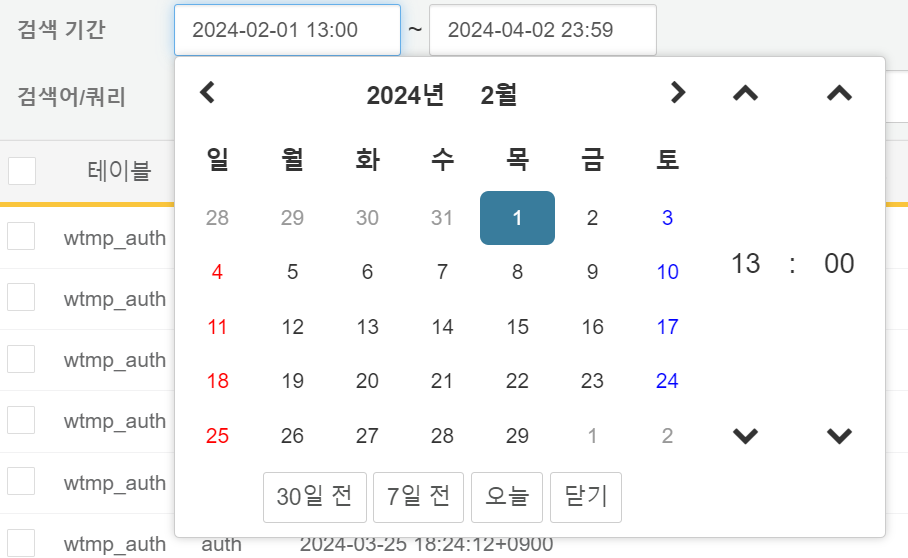
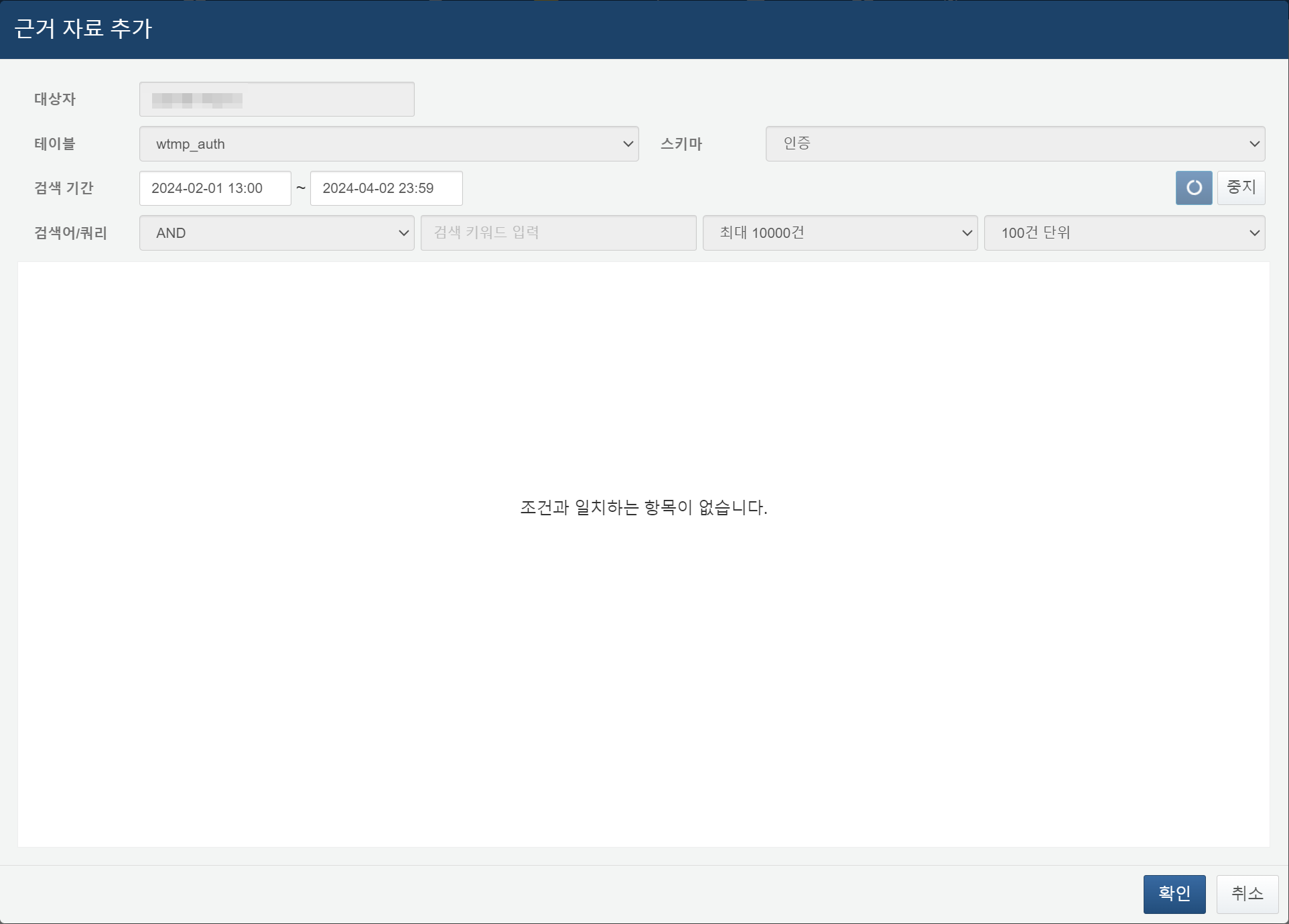
#### SNR#2471 티켓 태그를 수정하는 REST API 및 플레이북 명령 추가

티켓 태그를 수정하는 REST API 및 플레이북 명령을 추가했습니다.

* REST API: [티켓 태그 수정](https://docs.logpresso.com/ko/sonar/4.0/releases/ko/sonar/4.0/api/update-ticket-tags)
* 플레이북 명령
* 

#### SNR#1878 소명 요청 화면 사용자 인터페이스 개선

소명 요청 화면에서 근거 자료 관련 UI에 다음 개선사항이 반영되었습니다.

* 검색 기간 입력창에서 분리되어 있던 날짜와 시간 항목을 병합했습니다.
* 근거 자료 조회 시 "검색" 버튼에 조회중 아이콘을 표시합니다.
* 근거 자료 조회 시 입력창들이 비활성화됩니다.
* 근거 자료 조회 시 "중지" 버튼이 비활성화되는 문제를 해결했습니다.

#### SNR#1953 티켓에 대한 소명 요청 시 대상자 자동 할당

티켓 상세 화면에서 소명 요청할 때 티켓 근거자료에 사번(emp\_key) 필드가 있으면 해당 사번을 가진 임직원을 자동으로 소명 대상자로 지정하는 기능을 추가했습니다.

#### SNR#1954 소명 화면에 소명 대상자, 검토자 표시

소명 목록 화면에 소명 대상자, 1차 검토자, 2차 검토자 항목이 추가됐습니다.

소명 상세 화면에 소명 대상자, 1차 검토자, 2차 검토자 항목이 추가되고 소명 요청일 항목이 제거됐습니다.

#### SNR#1983 메일 서버 설정을 누락한 상태에서 소명 메일 발송 시 NullPointerException 예외 발생하는 문제 해결

메일 서버 설정을 하지 않은 채로 소명 메일을 발송하면 NullPointerException 오류 로그가 발생하던 문제를 해결했습니다. 패치 후에는 메일을 보내지 못한 이유를 알려주는 경고 로그가 발생합니다.

* 패치 후 - 웹 접속 주소 설정 시
* [2024-04-02 17:30:44.964] ERROR (ExplanationService) - sonar core: smtp server is not configured [2024-04-02 17:30:44.964] INFO (ExplanationService) - sonar core: send explanation request to employee [\*\*\*] for category [악성코드감염]
* 패치 후 - 웹 접속 주소 미설정 시
* [2024-04-02 17:29:07.170] WARN (ExplanationService) - sonar core: explanation domain not found. ignored email explanation request notification for employee [\*\*\*] [2024-04-02 17:29:07.170] INFO (ExplanationService) - sonar core: send explanation request to employee [\*\*\*] for category [악성코드감염]
* 패치 전 오류 로그
* [2024-04-02 17:21:06.445] ERROR (ExplanationService) - sonar core: cannot send explanation request notification mail, employee [\*\*\*] email [\*\*\*@logpresso.com] java.lang.NullPointerException at com.logpresso.sonar.api.impl.SmtpServiceImpl.\_\_M\_getMailerConfig(SmtpServiceImpl.java:177) at com.logpresso.sonar.api.impl.SmtpServiceImpl.getMailerConfig(SmtpServiceImpl.java) at com.logpresso.sonar.api.impl.ExplanationServiceImpl.\_\_M\_sendPrefixedExplanationRequestMail(ExplanationServiceImpl.java:938) at com.logpresso.sonar.api.impl.ExplanationServiceImpl.sendPrefixedExplanationRequestMail(ExplanationServiceImpl.java) ...

#### SNR#1998 자동/수동 소명 마감시한을 자정으로 통일

탐지 시나리오에서 자동으로 생성된 소명은 마감시한이 티켓 생성 시간을 기준으로 하고 사용자가 직접 생성한 소명 요청 마감 시한은 23:59:59인 문제가 있었습니다. 두 경우 모두 마감 시한을 자정(23:59:59)로 통일했습니다.

#### SNR#2286 소명 전용 웹 포트 분리

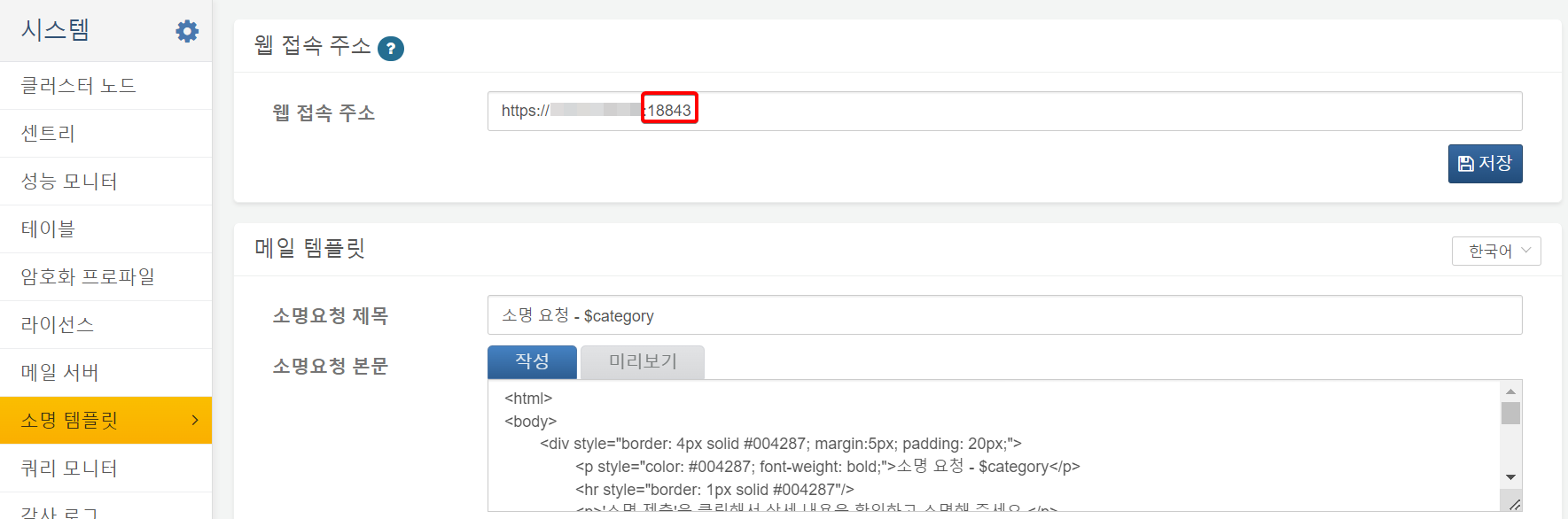
로그프레소 서버의 TCP 18443 포트에 접속할 수 있도록 방화벽 정책 설정을 변경하세요.

TCP 18443 포트를 소명 전용으로 사용하도록 새로 개방했습니다. 이전에는 임직원이 소명 작성 및 검토에 사용하는 웹 서버 포트가 웹 콘솔과 동일했지만, 보안 담당자 이외의 임직원이 웹 콘솔 접속을 시도할 가능성이 있으므로 소명 웹 포트를 분리하는 것이 보안 관리 측면에서 바람직합니다. 다만 업그레이드 시에는 구성을 변경하지 않고 기존 웹 포트에서 소명 접수를 처리할 수 있습니다.

소명 포트 번호를 별도로 지정하지 않은 경우 **18443** 포트를 사용하며, logpresso.sonar.explanation\_port 시스템 스위치를 사용하여 다른 포트 번호를 지정할 수 있습니다.

# 12345 포트를 소명 엔드포인트 포트로 사용-Dlogpresso.sonar.explanation\_port=12345

소명 포트를 지정한 경우 소명 템플릿에서 웹 접속 주소에 해당 포트를 명시해야 합니다.

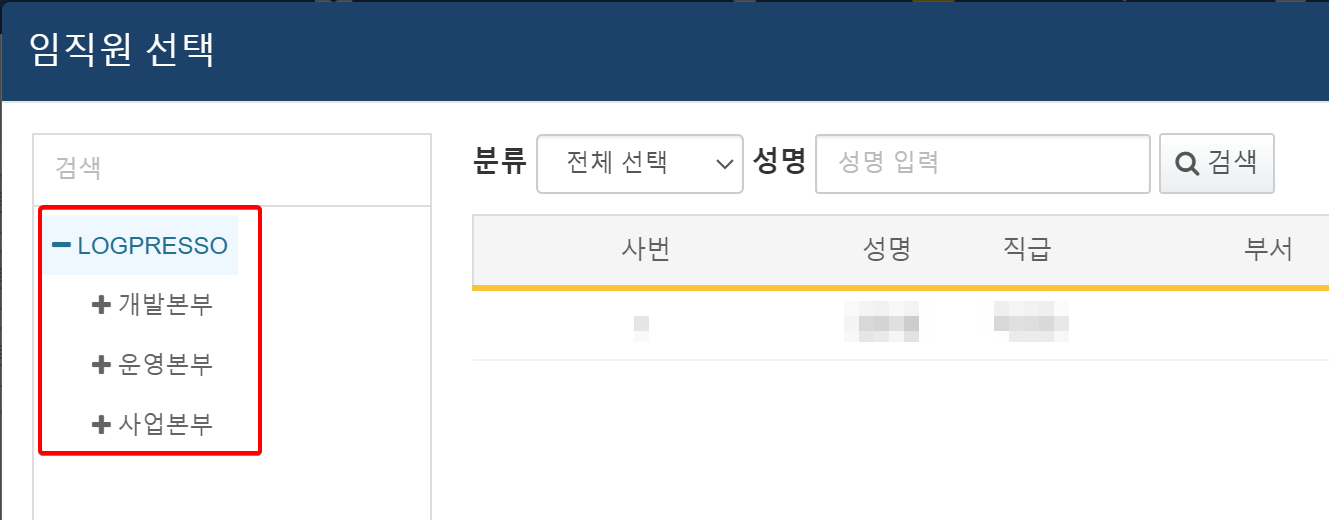


#### SNR#2308 소명 조회 시 행위 기간에 티켓 탐지 일시가 잘못 표시되는 문제 해결

소명 조회 시 행위 기간 항목에 실제 행위 시각이 아니라 티켓 탐지 시각이 표시되는 문제를 해결했습니다.

#### SNR#2349 소명 요청 화면의 임직원 선택 창에서 부서 트리를 최상위 단계로 축소 표시하도록 수정

소명 요청 화면에서 임직원 선택 창을 열었을 때 좌측의 부서 트리가 전부 펼쳐진 상태로 표시하지 않고 최상위 단계만 펼쳐지도록 수정했습니다.



#### SNR#2446 임직원 선택 창에 부서 검색 창 추가

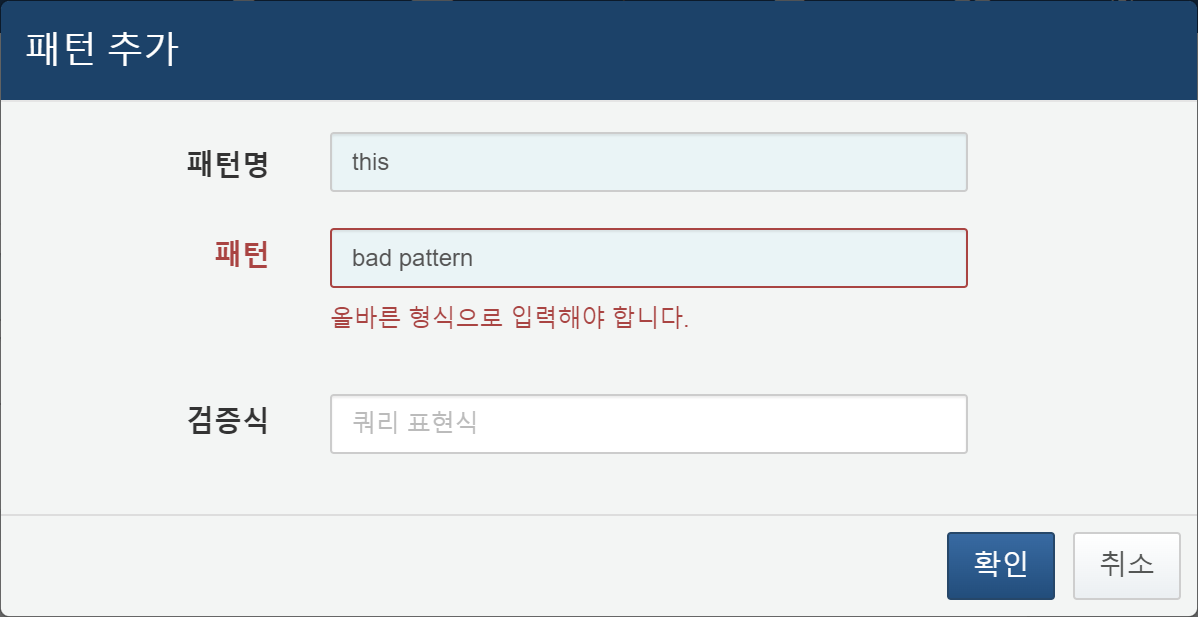
소명 요청 메뉴에서 임직원 선택 시 좌측에 표시되는 부서 트리에 부서 검색 창을 추가했습니다.

#### SNR#1833 실시간 탐지 시나리오 빌더 개선

실시간 탐지 시나리오 빌더 화면에 입력 값 검증 추가, 중복 표시 항목 제거, 잘못 표시된 항목 수정 등 개선 사항이 반영되었습니다.

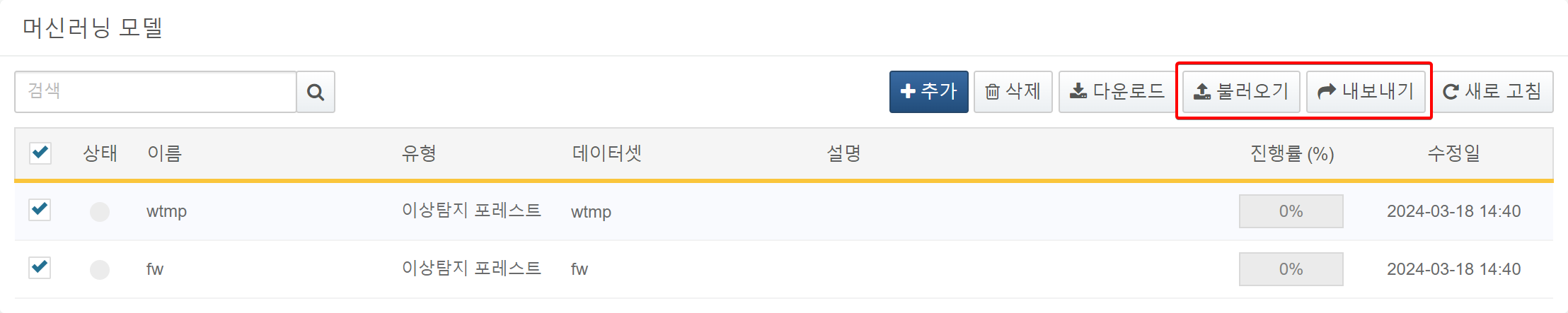
#### SNR#2015 웹 콘솔에서 패턴 추가 시 유효성 검사 수행

기존 버전에서는 웹 콘솔에서 패턴 추가 시 잘못된 패턴이나 검증식을 입력한 경우 패턴을 추가할 수 없다는 메시지만 표시되어서 어느 부분이 잘못 되었는지 파악할 수 없고, 웹 콘솔에서 입력한 내용이 전부 삭제되어 다시 입력해야 하는 문제가 있었습니다. 업그레이드 후에는 팝업 창에서 패턴 추가를 할 수 있으며, 어느 항목을 잘못 입력했는지 확인할 수 있습니다.



#### SNR#2181 머신러닝 모델 내보내기/불러오기 기능 추가

머신러닝 모델 내보내기/불러오기 기능이 추가되었습니다. 머신러닝 모델 파일 확장자는 .mlmodel입니다. 머신러닝 불러오기 대화상자에서 파일 목록은 .mlmodel 확장자를 가진 파일만 보여줍니다.



#### SNR#2231 자산 IP 목록 다운로드 시 사이트 항목 필터가 반영되지 않는 문제 해결

자산 IP 목록 다운로드 시 사이트 항목 필터가 반영되지 않고 모든 사이트의 데이터가 포함되는 문제를 해결했습니다.

#### SNR#2312 시나리오 분류 관리 메뉴에 삭제 버튼 추가

시나리오 분류 관리 화면에 삭제 버튼이 추가됐습니다.

#### SNR#2370 배치 시나리오 실행 시 표시되지 않던 오류 로그 추가

기존에 오류가 발생하더라도 오류 로그를 표시하지 않던 항목(예: 티켓 발생 실패)에 대해 오류 로그를 표시하도록 수정했습니다.

#### SNR#2410 알람 그룹에 계정 그룹을 하나만 할당해도 모든 계정 그룹이 할당된 것으로 보이는 문제 해결

알람 그룹에 계정 그룹을 할당한 후 다시 알람 그룹을 조회하면 모든 계정 그룹이 해당 알람 그룹에 할당된 것처럼 보이는 문제를 해결했습니다. 실제로는 설정한 계정 그룹만 할당되어 있었으나 화면에서는 모든 알람 그룹이 할당된 것으로 출력되었습니다. 알람 그룹에 실제 할당된 계정 그룹만 출력되도록 수정했습니다.

#### SNR#2419 실시간 탐지 시나리오 목록에서 분류 필터가 동작하지 않는 문제 해결

실시간 탐지 시나리오 목록에서 분류 항목에 대해 검색이 적용되지 않던 문제를 해결했습니다.

#### SNR#2477 실시간 시나리오 불러오기가 실패하는 문제 해결

구 버전에서 내보낸 실시간 시나리오를 로그프레소 셸에서 sonar.importStreamRules 명령으로 가져오면 Priority 타입 변경으로 인해 불러오기가 실패하여 아래와 같은 오류 로그가 발생하던 문제를 해결했습니다.

[2023-12-14 11:40:38,908] INFO (ScriptRunner) - araqne core: user [root] execute command [sonar.importStreamRules stream\_rule.json][2023-12-14 11:40:38,919] ERROR (ExchangeScript) - sonar exchange: cannot import stream rules from stream\_rule.jsonjava.lang.ClassCastException: class java.lang.String cannot be cast to class java.lang.Integer (java.lang.String and java.lang.Integer are in module java.base of loader 'bootstrap') at com.logpresso.sonar.api.exchange.impl.RuleExchangeServiceImpl.\_\_M\_importStreamRule(RuleExchangeServiceImpl.java:304) at com.logpresso.sonar.api.exchange.impl.RuleExchangeServiceImpl.importStreamRule(RuleExchangeServiceImpl.java) at com.logpresso.sonar.api.exchange.impl.RuleExchangeServiceImpl.\_\_M\_importStreamRules(RuleExchangeServiceImpl.java:223) at com.logpresso.sonar.api.exchange.impl.RuleExchangeServiceImpl.importStreamRules(RuleExchangeServiceImpl.java) at com.logpresso.sonar.api.exchange.impl.ExchangeScript.importStreamRules(ExchangeScript.java:165) ...

#### SNR#2322 실행 중인 플레이북 수정 시 자동 대응 내역 및 티켓 태스크 조회, 승인 동작이 실패하는 문제 해결

실행 중인 플레이북을 수정하면 다음 오동작들이 발생하던 문제를 해결했습니다.

* 자동 대응 내역 화면에서 실행 중인 플레이북 조회 및 실행 중단이 실패하는 문제
* 티켓 화면의 태스크 탭에서 플레이북 실행 내역이 표시되지 않는 문제
* 승인 요청 화면에서 실행 중인 플레이북에 대한 승인 처리를 할 수도 없고 삭제도 할 수 없는 문제

#### SNR#2376 플레이북 목록에서 "시작 유형"이 새 사이트로 표시되는 문제 해결

4.0.2308.0 버전 이후 플레이북 목록에서 "시작 유형"이 새 사이트로 표시되는 문제를 해결했습니다.

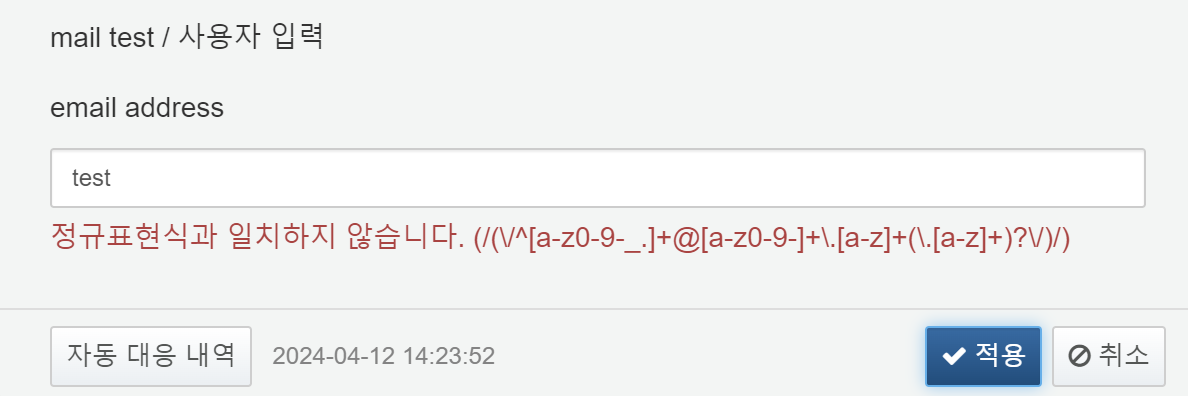
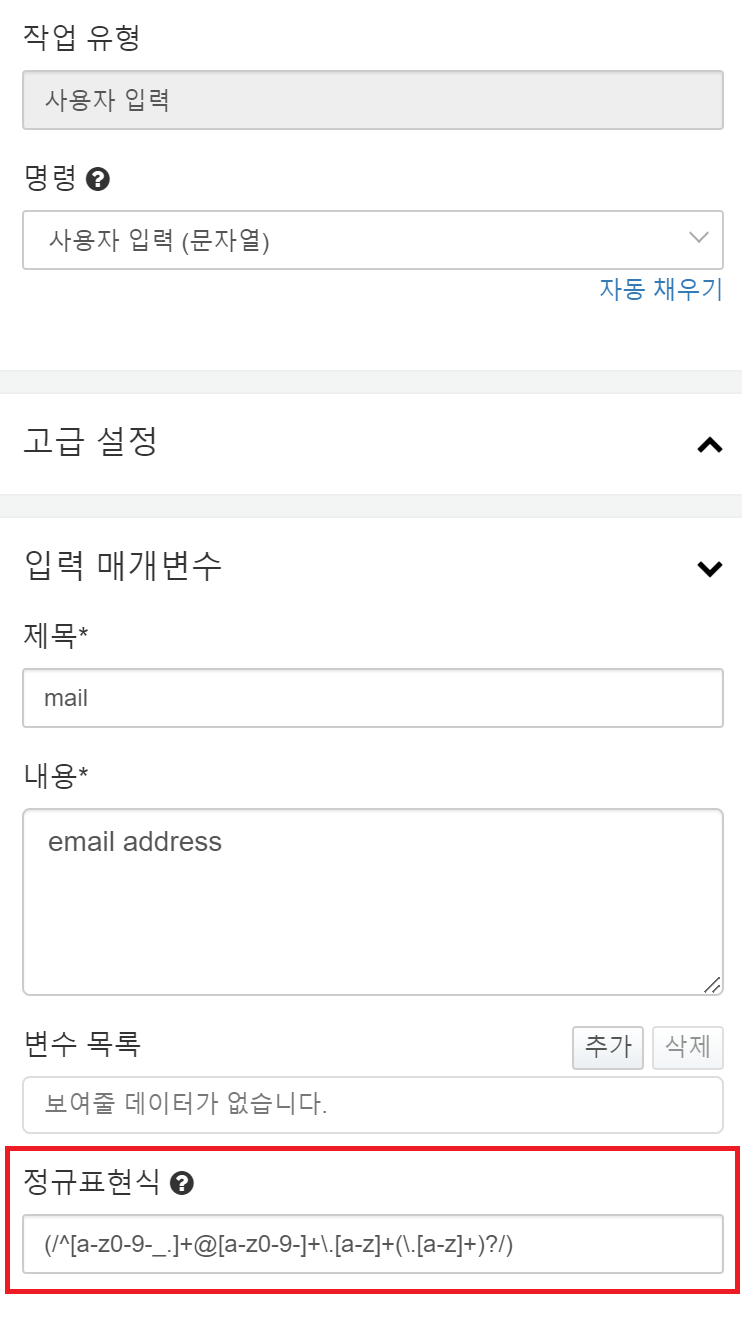
#### SNR#2420 플레이북 관련 버그 및 개선 사항

플레이북에서 다음과 같은 버그 해결 및 개선 사항이 있었습니다.

* 사용자 입력 중에서 "(논리형) 입력" 항목이 예/아니오 라디오 버튼으로 표시됩니다.
* 사용자 입력/승인 요청 내역을 표시할 때 줄바꿈이 적용됩니다.
* 플레이북 복제 시 비활성화 상태로 복제됩니다.
* 실행 완료된 플레이북을 삭제한 뒤 자동 대응 내역을 조회할 때 NullPointerException 예외가 발생하는 문제를 해결했습니다. 기존 오류 로그는 다음과 같습니다.
* [2024-03-25 17:36:11,489] ERROR (MessageBusImpl) - araqne msgbus: message handler failed java.lang.NullPointerException at com.logpresso.maestro.msgbus.PlaybookPlugin.\_\_M\_getPlaybookRun(PlaybookPlugin.java:571) at com.logpresso.maestro.msgbus.PlaybookPlugin.getPlaybookRun(PlaybookPlugin.java)

#### SNR#2426 플레이북 사용자 입력 태스크의 유효성 검사 옵션 추가

플레이북 사용자 입력 태스크에 입력값 유효성을 검사할 정규표현식을 추가할 수 있습니다.



#### SNR#2428 플레이북 태스크 "실패 허용" 옵션 추가

플레이북 태스크 옵션으로 "실패 허용" 옵션이 추가됐습니다. "실패 허용" 옵션을 설정한 경우 해당 태스크가 실패해도 플레이북이 종료되지 않고 다음 태스크로 넘어갑니다.

#### SNR#2454 플레이북 분기 태스크에 불리언이 아닌 표현식을 사용할 때 NullPointerException 예외 발생하는 문제 해결

플레이북 분기 태스크에 불리언(true, false)이 아닌 표현식을 사용할 때 NullPointerException 예외가 발생하며 태스크가 실패하는 문제를 해결했습니다. 패치 후에는 불리언이 아닌 표현식을 사용해도 NullPointerException 예외가 발생하지 않고 정상적으로 수행됩니다.

maestro core: playbook [플레이북 테스트\_20240409] task [분기] is completed with errorjava.lang.NullPointerException at com.logpresso.maestro.api.impl.DecisionTaskHandlerImpl.\_\_M\_handleExpression(DecisionTaskHandlerImpl.java:99) at com.logpresso.maestro.api.impl.DecisionTaskHandlerImpl.handleExpression(DecisionTaskHandlerImpl.java) at com.logpresso.maestro.api.impl.DecisionTaskHandlerImpl.\_\_M\_handleTask(DecisionTaskHandlerImpl.java:78) at com.logpresso.maestro.api.impl.DecisionTaskHandlerImpl.handleTask(DecisionTaskHandlerImpl.java)...

#### SNR#1976 암호 만료 기한을 7일로 설정하면 암호 변경을 해도 암호 변경 창이 계속 출력되는 문제 해결

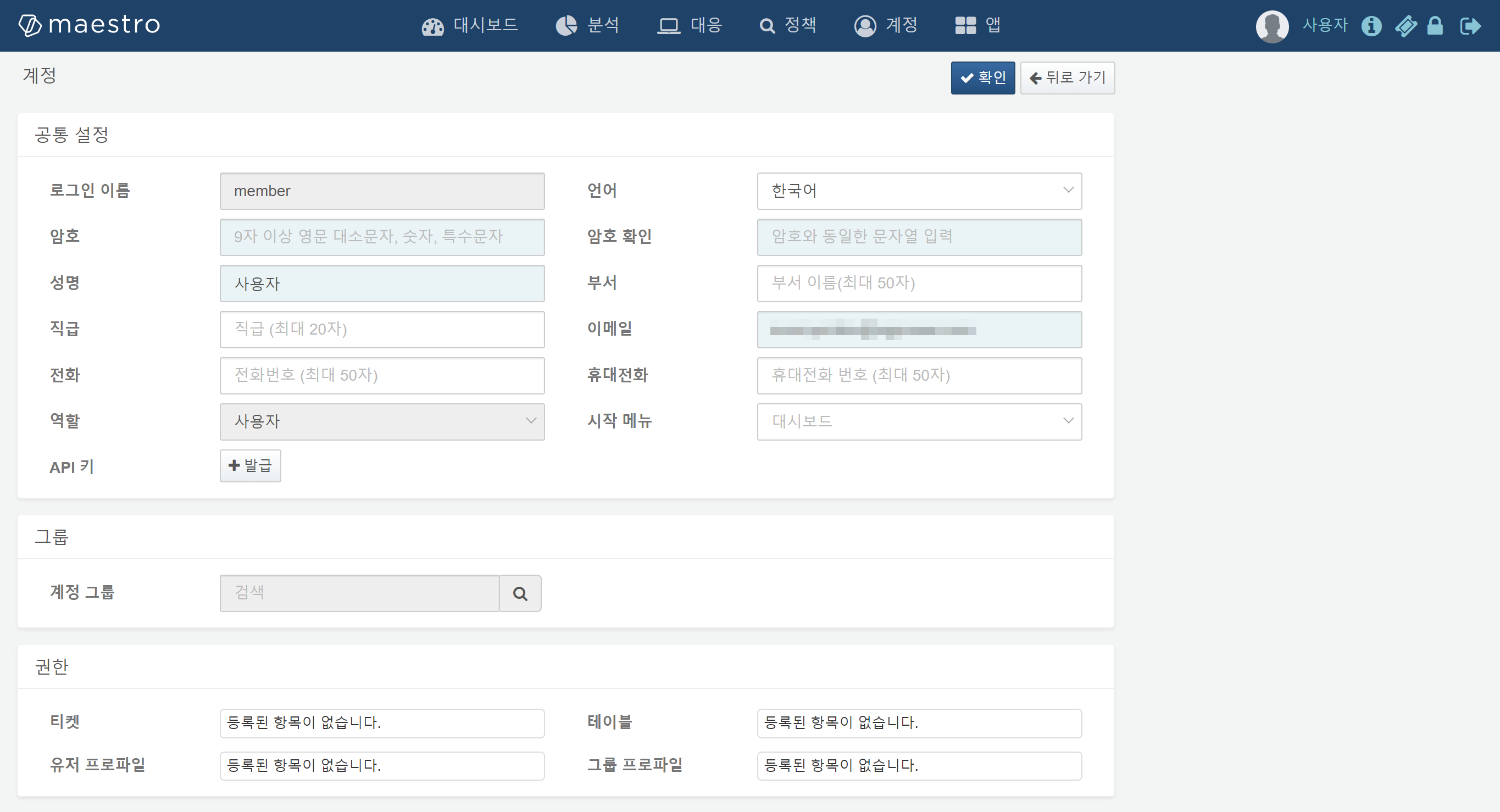
기존에는 암호 만료일이 7일 남은 상태에서 로그인했을 때 암호 변경 창이 출력됩니다. 암호 만료 기한을 7일로 설정하면 아무리 암호를 변경해도 만료일이 7일 남기 때문에 암호 변경 창이 계속 출력되는 문제가 있었습니다. 암호 만료일이 6일 남았을 때 암호 변경 창을 출력하도록 수정하여 문제를 해결했습니다.

#### SNR#2220 계정 추가 화면에서 역할 기본값을 사용자로 변경

최소 권한 원칙에 따라 계정 추가 화면에서 역할의 기본값을 클러스터 관리자에서 사용자로 변경했습니다.

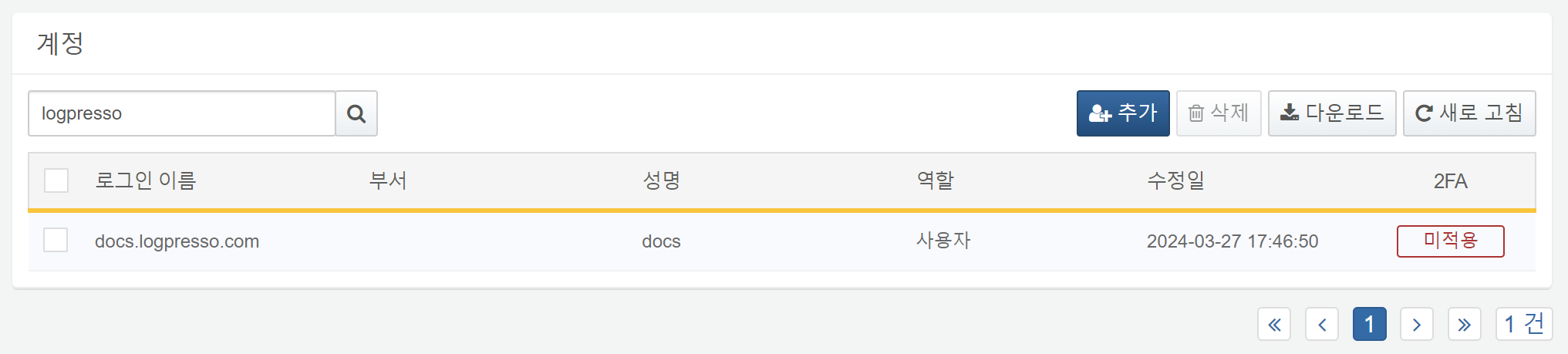
#### SNR#2226 사용자 권한 계정은 타 계정의 최소 정보만 접근하도록 보안 강화

티켓 할당, 결재 요청 등 업무 상 사용자 권한의 계정에서도 전체 계정 목록은 조회할 수 있어야 하나, 권한 등 계정의 세부 정보까지 조회하지 못하도록 보안을 강화하였습니다.

* 본인 정보 수정은 우상단 계정 아이콘을 클릭하여 가능

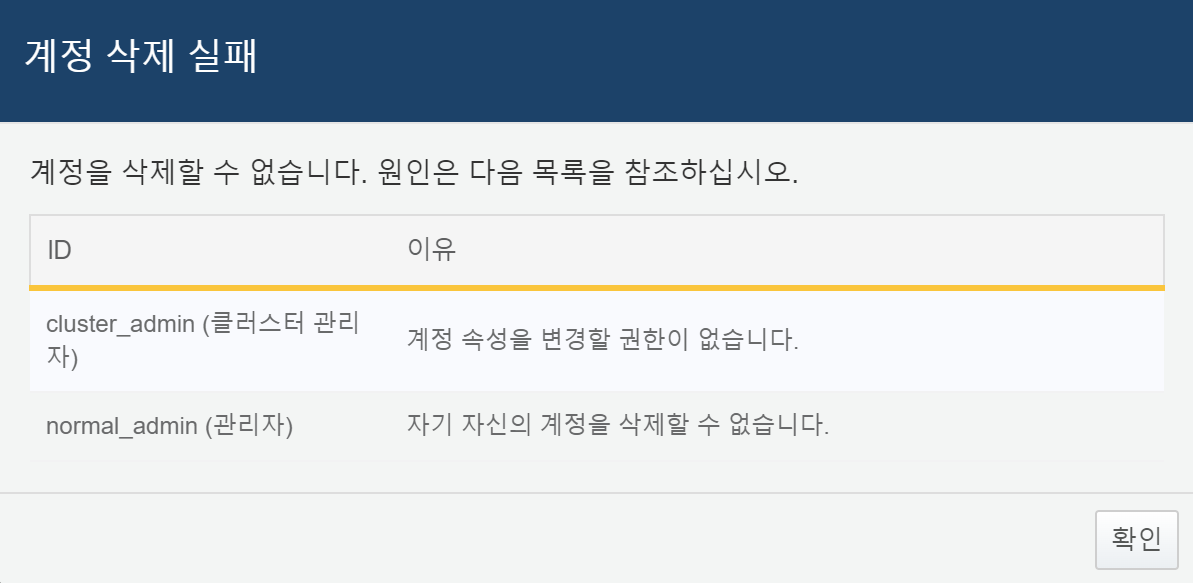
#### SNR#2377 로그인 계정 이름에 `.` 문자를 허용하도록 수정

액티브 디렉터리 등 외부 인증 연동 시 계정 이름에 . 문자가 포함된 경우가 존재합니다. 이에 따라 계정 관리 및 인스톨러 화면에서 계정 이름에 . 문자도 허용하도록 수정했습니다.



#### SNR#2403 관리자 권한으로 클러스터 관리자 계정 삭제 시도 시 삭제 실패임에도 성공 메시지가 출력되는 문제 해결

관리자 권한으로 클러스터 관리자 계정을 삭제 시도하면 클러스터 관리자 계정이 삭제되지 않았음에도 삭제했다는 메시지가 출력되는 문제를 해결했습니다.



#### SNR#2272 센트리 접속 상태 아이콘이 단절 상태(회색)에서 변경되지 않는 문제 해결

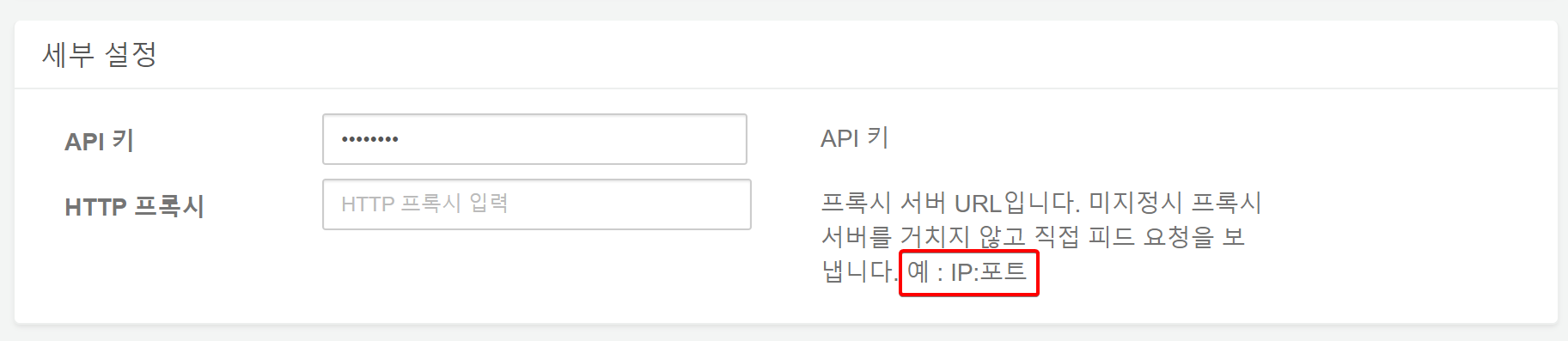
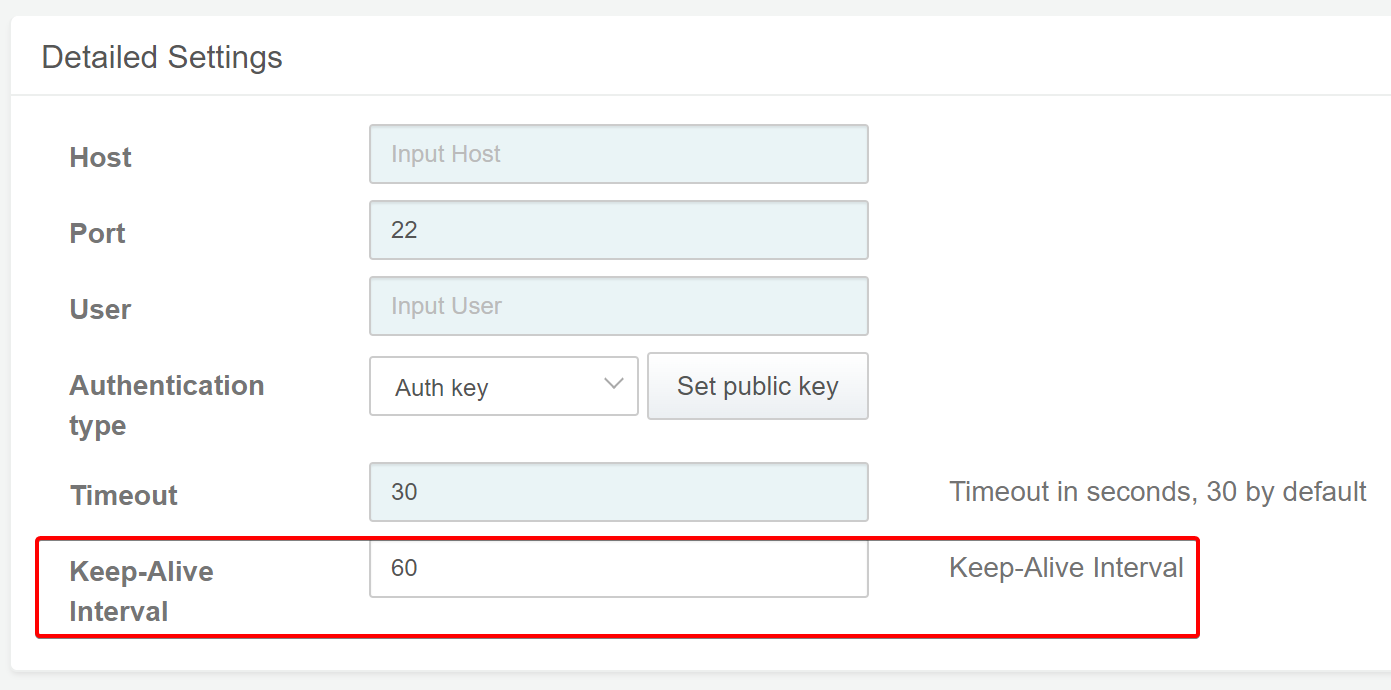
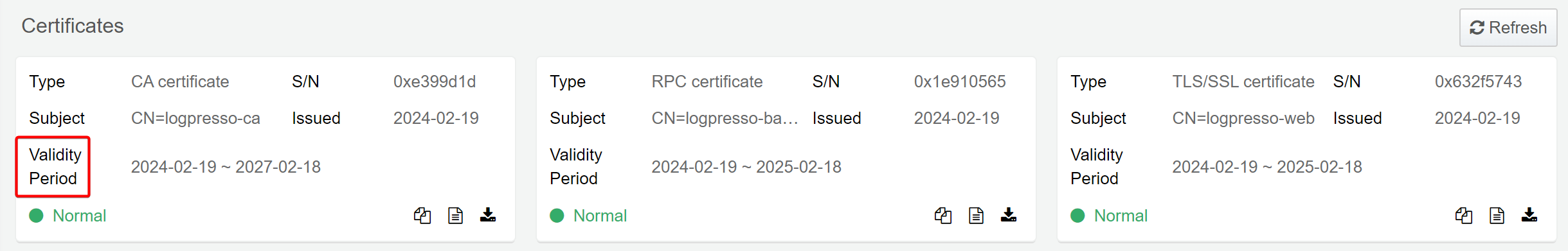
다음 상황이 발생할 경우, 센트리 목록에 표시되는 센트리 접속 상태 아이콘이 회색(단절)에서 녹색(접속)으로 변경되지 않는 문제를 해결했습니다.

* 최초 접속 시 센트리에서 성능 정보를 가져오지 못하는 경우
* 센트리 접속이 단절될 때 센트리와 서버의 시간이 다른 경우 (NTP 등의 이슈)

#### SNR#2348 메일 서버 프로토콜이 포트 번호에 따라 결정되는 문제 해결

메일 서버 설정 시 선택한 프로토콜과 무관하게 포트 번호에 따라 프로토콜이 결정되는 문제를 해결했습니다. 이전에는 포트 번호를 587로 입력하면 프로토콜은 무조건 TLS로 설정되었고, 465로 입력하면 SSL로 설정되었습니다. 패치 후에는 사용자가 선택한 프로토콜을 적용합니다.

#### SNR#2366 접속 프로파일, 인증서 관련 웹 콘솔 메시지 수정

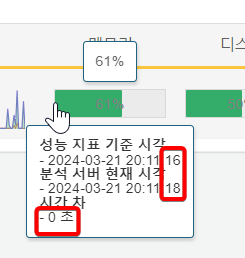
* Logpresso CTI 접속 프로파일의 "HTTP 프록시" 설명을 수정했습니다.
* 수정 전: "프록시 서버 URL입니다. 미지정시 프록시 서버를 거치지 않고 직접 피드 요청을 보냅니다. 예: http://HOST:PORT"
* 수정 후: "프록시 서버 URL입니다. 미지정시 프록시 서버를 거치지 않고 직접 피드 요청을 보냅니다. 예: IP:포트"
* SSH 접속 프로파일 "접속 유지 시간"에 해당하는 영문을 수정했습니다.
* 수정 전: Server Alive Interval
* 수정 후: Keep-Alive Interval
* 인증서 화면에서 "유효 기간"에 해당하는 영문을 수정했습니다.
* 수정 전: End of valid
* 수정 후: Validity Period

#### SNR#2401 차단 연동 세부설정 화면에서 드롭다운 항목의 표시 이름과 값이 뒤바뀌는 문제 해결

차단 연동 세부설정 화면에서 드롭다운 항목을 표시할 경우 표시 이름 대신 값이 출력되고, 설정 시 드롭다운 항목의 값 대신 표시 이름이 설정되는 문제를 해결했습니다.

#### SNR#2434 성능 모니터에서 각 지표의 시간 차가 항상 0초로 표시되는 문제 해결

성능 모니터에서 성능 지표 기준 시각과 서버 현재 시각의 시간 차 값이 항상 0초로 표시되는 문제를 해결했습니다.



#### SNR#2448 설치 직후 테이블 메뉴 조회 시 NullPointerException 발생하는 문제 해결

설치 직후 테이블 메뉴를 조회할 경우 아래와 같이 NullPointerException 예외가 발생하는 문제가 해결됐습니다.

[2024-01-17 17:25:02,601] ERROR (MessageBusImpl) - araqne msgbus: message handler failedjava.lang.NullPointerException at com.logpresso.sonar.dom.impl.TableServiceImpl.\_\_M\_getCompanyTotalDiskUsage(TableServiceImpl.java:493) at com.logpresso.sonar.dom.impl.TableServiceImpl.getCompanyTotalDiskUsage(TableServiceImpl.java) at com.logpresso.sonar.dom.impl.TableServiceImpl.\_\_M\_getTables(TableServiceImpl.java:482) at com.logpresso.sonar.dom.impl.TableServiceImpl.getTables(TableServiceImpl.java) ...

#### SNR#2451 최초 설치 시 클러스터 노드의 인증서 검증 설정이 활성화되는 문제 해결

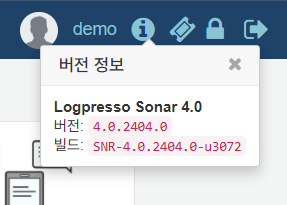
최초 설치 시 클러스터 노드 설정의 인증서 검증 설정이 활성화되어 생성되는 문제가 있었습니다. 기본 노드 설정에서 주소가 127.0.0.1로 세팅되어 있어서 문제가 발생하지 않았으나 정책 동기화 주소 설정 시 (sonar.setMaster)에서 다른 IP 주소를 입력할 경우 연결이 되지 않는 문제가 있었습니다. 패치 후 신규 설치 시 인증서 검증 설정이 비활성화되었습니다.

#### SNR#2456 성능 모니터에서 GC 지표 문구 수정

성능 모니터링 화면의 GC 지표 문구 중 "실패"를 "경고"로 변경했습니다.

#### SNR#1463 웹 콘솔 대메뉴에 제품 버전 정보 표시

웹 콘솔 대메뉴에서 i 아이콘을 누르면 현재 제품 버전이 표시됩니다. 기존에 있던 "내 정보" 아이콘은 내 계정 아이콘 또는 이름을 클릭하는 것으로 대체되었습니다.



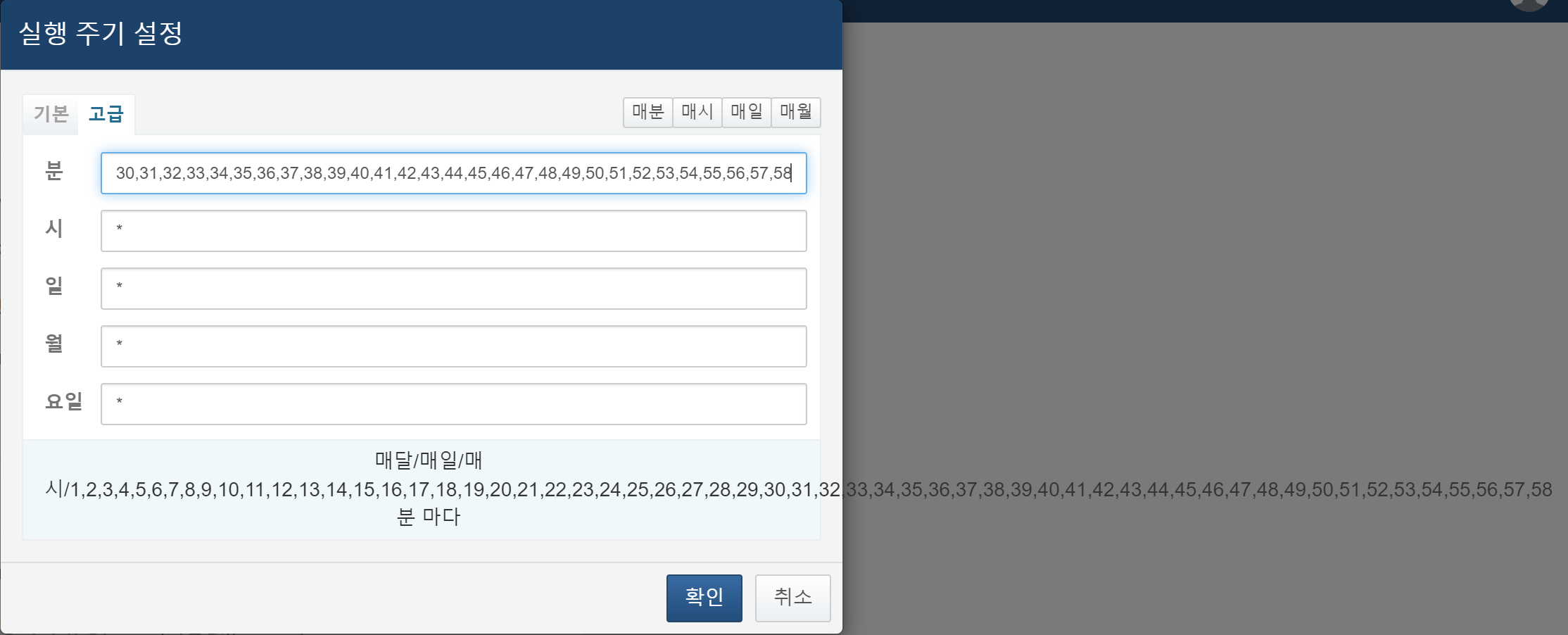
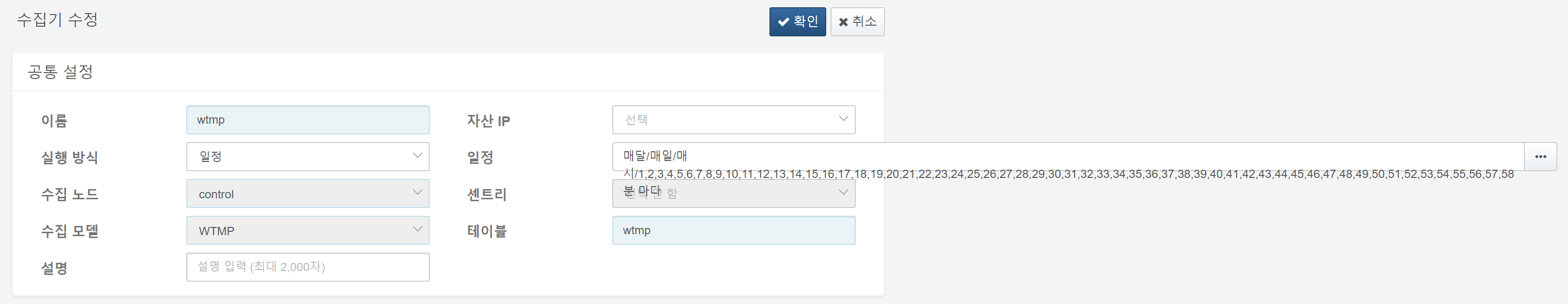
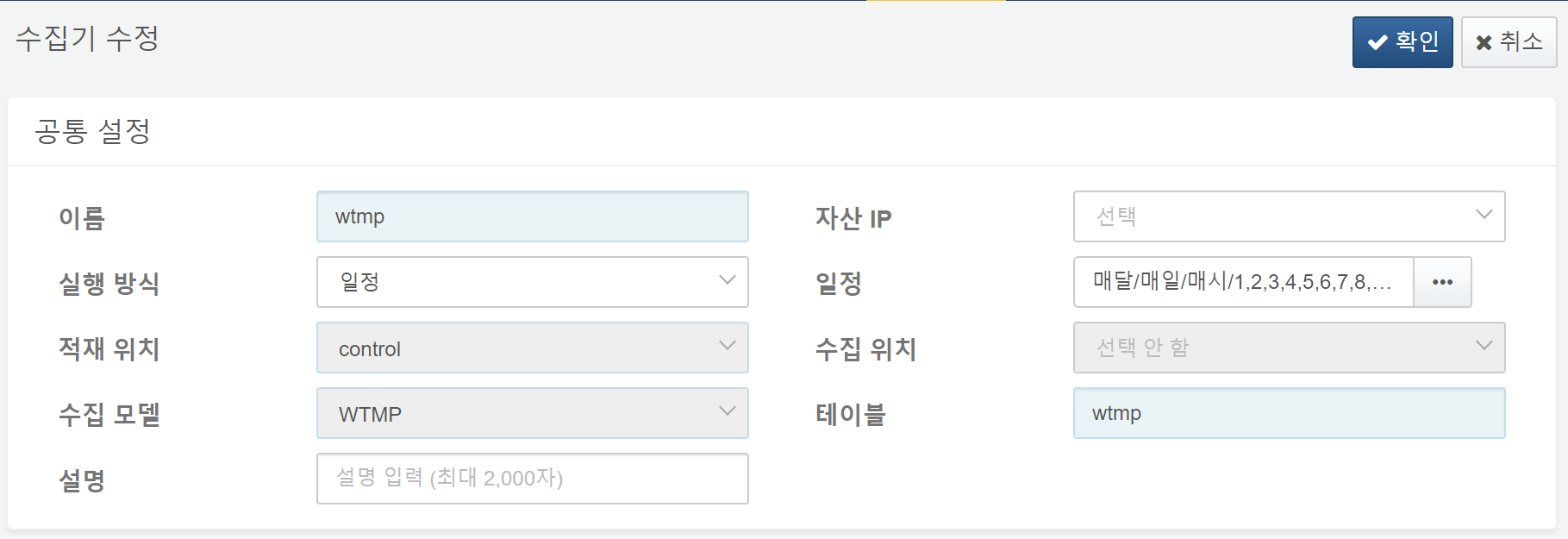
#### SNR#1690 수집기, 예약된 쿼리, 배치 시나리오 일정 입력 시 긴 입력값 및 복합 일정 입력 지원

일정 설정 화면에서 긴 입력값을 처리하지 못하는 문제와 복합 일정을 입력하지 못하는 문제를 해결했습니다. 영향 받는 기능은 다음과 같습니다.

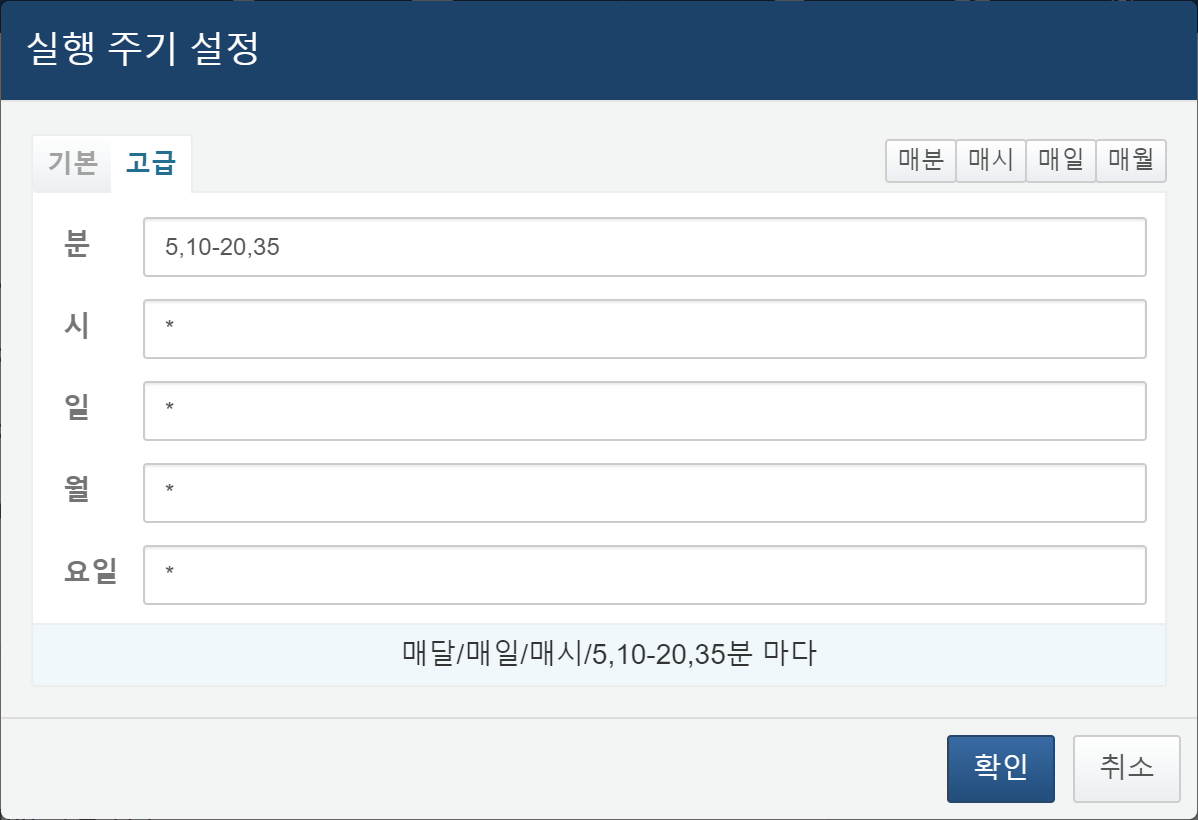
* 수집기
* 예약된 쿼리
* 배치 탐지 시나리오

변경 사항은 다음과 같습니다.

일정 설정 화면에서 입력값이 너무 길면 화면 레이아웃이 깨지고 입력 오류가 발생하여 설정을 저장할 수 없는 문제가 해결됐습니다.

* 패치 전: 화면 레이아웃이 깨지고 저장이 되지 않는 문제
* 
* 
* [2024-03-14 18:23:19.278] ERROR (MessageBusImpl) - araqne msgbus: message handler failed java.lang.IllegalStateException: sonar sql [UPDATE sonar\_loggers SET name = ?, ip\_id = ?, configs = ?, description = ?, `interval`=?, schedule=?, updated\_at=? WHERE id = ?] failure at com.logpresso.sonar.dom.impl.SqlConnectorImpl.\_\_M\_execute(SqlConnectorImpl. java:268) at com.logpresso.sonar.dom.impl.SqlConnectorImpl.execute(SqlConnectorImpl.java) at com.logpresso.sonar.api.impl.LoggerServiceImpl.\_\_M\_updateLogger (LoggerServiceImpl.java:1558) at com.logpresso.sonar.api.impl.LoggerServiceImpl.updateLogger (LoggerServiceImpl. java) ... Caused by: java.sql.SQLDataException: (conn=3202) Data too long for column 'schedule' at row 1 ... at com.logpresso.sonar.msgbus.LoggerPlugin.\_\_M\_updateLogger(LoggerPlugin.java:748) at com.logpresso.sonar.msgbus.LoggerPlugin.updateLogger(LoggerPlugin.java) ... Caused by: java.sql.SQLException: Data too long for column 'schedule' at row 1 ...
* 패치 후: 화면 정상적으로 표시
* 
* 

5,10-20,35과 같이 복잡한 형태의 일정을 입력할 수 없던 문제를 해결했습니다.



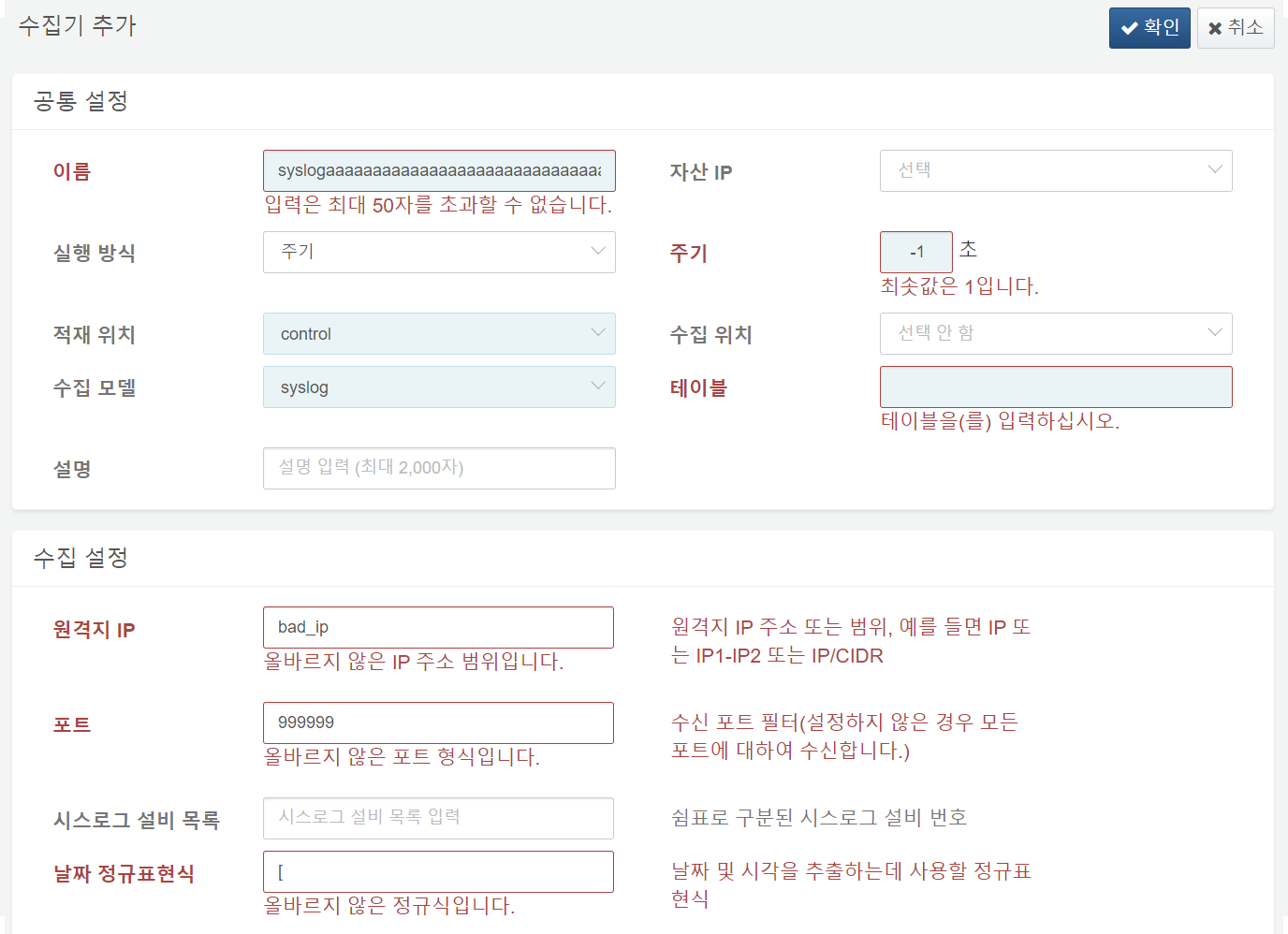
#### SNR#2248 제품 전반에 걸친 웹 콘솔 사용성 개선 및 버그 수정

* 공통
* 화면 잠금 해제 시 탐지 현황, 수집기 목록 화면이 계속 불러오는 중 상태로 남아있는 문제 해결
* 수집기 그룹 또는 임직원 부서 선택 후 항목 추가 시 선택된 그룹/부서에 포함되어 생성되도록 개선
* 체크박스 목록 전체 선택 후 일부 해제 시 전체 선택 해제가 되지 않는 문제 해결
* 수집
* 수집 주기 최댓값을 1,000,000초로 변경
* 수집 관련 항목 삭제 실패 창 일관성 개선
* 수집 모델에서 정규화 규칙 추가 시 정규화 규칙의 로그 스키마가 표시되지 않는 문제 해결
* 파서 목록 다운로드 시 로그 스키마 관련 필드 삭제
* 파서 식별자에 공백 입력 방지
* 로그 스키마 코드를 이름과 함께 표시하도록 개선
* 스키마 추가 시 라벨과 플레이스홀더를 "식별자"로 통일
* 분석
* 데이터셋 연관 분석 설정 시 이름이나 쿼리문이 긴 경우에 대한 처리 추가
* 데이터셋/쿼리 불러오기 대화상자에 긴 텍스트 처리 추가
* 학습 데이터셋 편집 시 이름을 변경하지 않아도 이름이 중복이라고 표시되는 문제 해결
* 이벤트 필터 시 "IP 블랙리스트"로 표시된 항목을 "주소 그룹"으로 변경
* 로그 및 쿼리 화면에서 쿼리 결과 저장 시 알림 토스트 메시지를 표시하도록 수정
* 탐지 현황 목록에서 테스트 필드 제거
* 프로시저 공유 설정 개선
* 대응
* 차단 내역 목록의 대응 필드에 값이 표시되지 않는 문제 해결
* 티켓
* 티켓 목록 다운로드 화면에서 등록자가 "등록"으로 표시되는 문제 해결
* 결재자가 반려한 티켓을 담당자가 다시 처리 중으로 변경 시 티켓 상태가 "처리 중"으로 표시되도록 수정
* 티켓에 띄어쓰기 없이 제목 입력 시 텍스트가 테이블 밖으로 나가는 문제 해결
* 티켓에 할당자로 할당된 계정이 삭제된 경우 null로 표시되는 문제 해결
* 태그 이름에 공백이 연속으로 여러 개 있어도 1개만 표시되는 문제 해결
* 티켓 목록 표시 개수 변경 시 알림 메시지가 2번 뜨는 문제 해결
* 태그 목록 다운로드 시 소유자 필드 제거
* 탐지 시나리오
* 실시간 시나리오 빌더에서 필수 항목을 입력하지 않아도 "추가" 버튼이 활성화되는 문제 해결
* 실시간 시나리오 빌더 화면 레이아웃이 깨지는 문제 해결
* 위협 탐지로 인한 알람 메일 이미지 개선
* 티켓 화면에서 SMS 상황전파 시 알람이 전송되지 않는 문제 해결
* 로그 스키마 필드 타입에 대한 시나리오 빌더 처리 개선
* 시나리오 분류 추가 화면에서 플레이스홀더 설명 개선
* 시나리오 분류 이름이 긴 경우 설명과 겹치는 문제 해결
* 배치 탐지 시나리오 추가/수정 화면 제목 수정
* 시나리오 빌더에서 "대상 값 범위" 선택 시 시작값과 끝값이 같은 값으로 설정되는 문제 해결
* 배치 시나리오 설정 화면에서 주소 그룹을 선택 안 할 경우 항목 이름을 "선택 안 함"으로 통일
* 정책
* 추가, 수정 메뉴 제목 통일 (예: "새 사이트"는 "사이트 추가", "포트 그룹 편집"은 "포트 그룹 수정"으로 변경)
* 클러스터 노드 추가 화면에서 기본으로 입력되어 있는 값 개선
* 노드 화면 메시지 개선
* 포트 그룹 검색 시 오류 로그 발생하는 문제 해결
* 패턴 그룹 항목 추가 화면 개선
* 자산 IP 화면에서 긴 호스트명 입력 시 삭제 팝업 창에 표시되는 텍스트가 벗어나는 현상
* 행위 프로파일 수정 화면에서 쿼리문 항목 비활성화
* 머신러닝 모델에서 학습 데이터셋 입력 필드를 선택하지 않은 경우 모델 필드 테이블이 표시되지 않는 문제 해결
* 네트워크 대역 항목 추가 팝업에서 유형 항목 창 길이 수정
* 계정
* 윈도우 알림 창에 중복 로그인 알람이 뜨는 문제 해결
* 관리자 권한 계정이 없으면 계정 삭제를 할 수 없는 문제 해결
* 관리자 계정으로 다른 관리자 계정 정보를 수정할 수 없는 문제 해결
* 암호 변경 시 기존 암호를 재사용하려 할 경우 오류 메시지 개선
* 관리자 권한 계정으로 포트 그룹 내의 포트 정보 추가/수정/삭제가 안되는 문제 해결
* 시스템
* 암호 만료 기간을 7일 이하로 설정 시 암호를 변경해도 암호 만료 창이 닫히지 않는 문제 해결
* 차단 연동 설정 화면에서 차단 연동 모델이 없거나 해당하는 프로파일이 없을 경우 프로파일 드롭다운을 표시하지 않도록 수정
* 사용 중인 암호화 프로파일 삭제 시 삭제 실패 메시지가 표시되지 않는 문제 해결
* 테이블
* 테이블 삭제 시 삭제 확인 메시지 추가
* 수집기에서 사용하고 있는 테이블 삭제 시도 시 오류 메시지 개선

#### SNR#2250 객체 생성 및 편집 시 입력값 유효성 검증 개선

소나 객체 생성 및 편집 시 입력값에 대한 유효성 검증을 개선했습니다. 변경사항은 다음과 같습니다.

* 이름 중복 방지
* 값 유형에 따른 유효성 검증 추가 (최대/최소 범위, 문자열 길이, 타입에 맞는 값 여부 등)
* 유효성 검증 실패 항목에 대한 표시 개선
* 누락되거나 잘못된 플레이스홀더 개선



#### SNR#2371 잘못된 쿠키 값이 설정된 경우 로그인 후 브라우저 새로고침 시 다시 로그인 창이 출력되는 문제 해결

브라우저에 기존에 잘못 세팅된 쿠키(cookie)가 남아있는 상태에서 소나 로그인 시 쿠키가 갱신되지 못하는 문제가 있었고, 이 때문에 로그인 후 브라우저를 새로고침 하면 로그인 상태를 인식하지 못해 다시 로그인 창이 뜨는 현상이 발생했습니다. 패치 후 쿠키 갱신을 정상적으로 하도록 수정되었습니다.

#### SNR#2417 쿠키 탈취 시도 시 NullPointerException 예외가 발생하는 문제 해결

동일 쿠키로 다른 IP 주소에서 접속 시도할 경우 쿠키 탈취 시도 로그를 남겨야 하는데 NullPointerException 예외가 발생하던 문제를 해결했습니다.

* 패치 전 DEBUG 로그
* [2024-03-13 16:16:23.336] DEBUG (LoginPlugin) - sonar core: relogin failed, cookie [a4caef7c-9afd-4551-98ae-cccdd718c670] java.lang.NullPointerException ... at com.logpresso.sonar.msgbus.LoginPlugin.\_\_M\_checkCookieSteal(LoginPlugin.java:358) at com.logpresso.sonar.msgbus.LoginPlugin.checkCookieSteal(LoginPlugin.java) at com.logpresso.sonar.msgbus.LoginPlugin.\_\_M\_reLogin(LoginPlugin.java:523) at com.logpresso.sonar.msgbus.LoginPlugin.reLogin(LoginPlugin.java) ...
* 패치 후 DEBUG 로그
* [2024-03-13 16:28:19.887] DEBUG (LoginPlugin) - sonar core: relogin failed, cookie [9758c1da-8d36-4e27-b96f-a0e4e7a8cad4] java.lang.IllegalStateException: cookie-stealing-detected at com.logpresso.sonar.msgbus.LoginPlugin.\_\_M\_checkCookieSteal(LoginPlugin.java:361) at com.logpresso.sonar.msgbus.LoginPlugin.checkCookieSteal(LoginPlugin.java) at com.logpresso.sonar.msgbus.LoginPlugin.\_\_M\_reLogin(LoginPlugin.java:523) at com.logpresso.sonar.msgbus.LoginPlugin.reLogin(LoginPlugin.java) ...

#### SNR#2425 REST API 경로에 포함된 매개변수가 URL 디코드 되지 않는 문제 해결

REST API가 경로를 통해 매개변수를 전달받는 경우 해당 매개변수 값이 URL 디코드 되지 않는 문제를 해결했습니다. 예를 들어 로그 스키마의 필드 표시 이름이나 룩업의 키 이름에 공백이 있어서 %20으로 전달된 경우 이를 공백으로 인식하지 못하는 문제가 있었습니다.

#### SNR#2431 날짜 선택기에서 1월 이전이나 12월 이후로 이동해도 연도가 바뀌지 않는 문제 해결

날짜 선택기에서 월 증가/감소 버튼을 클릭하여 1월 이전이나 12월 이후로 이동해도 연도가 바뀌지 않는 문제를 해결했습니다.

