## 릴리스 4.0.2308.0

### 알려진 이슈

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

**아래 이슈들은 4.0.2312.2 패키지에서 해결했습니다.**

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

### 메인 피쳐

|  |  |
| --- | --- |
| 식별자 | 항목 |
| [SNR#1612](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1612) | 다국어 로케일 지원 |
| [SNR#1761](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1761) | REST API 지원 |
| [SNR#2028](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2028) | 파서 및 수집 모델 UI 간소화 |
| [SNR#2029](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2029) | 성능 모니터 기능 추가 |
| [SNR#2038](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2038) | 멀티 테넌트 기능 파기 |
| [SNR#2044](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2044) | 사이트, 호스트명, 자산 태깅 기능 추가 |
| [SNR#2045](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2045) | 로그프레소 제품 단일 패키지화 및 라이선스 체계 변경 |
| [SNR#2055](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2055) | 스토리지 생명주기 지원 |
| [SNR#2068](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2068) | 단일 노드 구성에 대해 SQLite 백엔드 지원 |

### 신규 기능

|  |  |
| --- | --- |
| 식별자 | 항목 |
| [SNR#1773](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1773) | 시나리오 분류 관리 기능 추가 및 소명 분류 관리 화면을 팝업으로 변경 |
| [SNR#1782](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1782) | 휴면 계정 전환 기능 추가 |
| [SNR#1783](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1783) | 계정 최소 암호 길이 및 암호 재사용 방지 정책 설정 기능 추가 |
| [SNR#1947](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1947) | 보고서 및 다운로드 파일 형식에 PDF 포맷 추가 |
| [SNR#1962](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1962) | 티켓 일괄 작업 시 메모 입력 기능 추가 |
| [SNR#1965](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1965) | 티켓 태그 기능 추가 |
| [SNR#2011](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2011) | 사용자 정의 필터 객체 및 matchfilter 함수 지원 |
| [SNR#2080](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2080) | 테이블 데이터 복구 과정에서 데이터 파일 헤더가 손상되는 문제 해결 |
| [SNR#2105](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2105) | 수집기 필터 기능 추가 |
| [SNR#2122](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2122) | 앱 리소스 자동 설치 |
| [SNR#2126](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2126) | Syslog over TLS 수신 기능 추가 |
| [SNR#2135](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2135) | sonar-add-address-batch 명령어 추가 |
| [SNR#2136](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2136) | sonar api key 발급 기능 추가 |

### 기능 개선

|  |  |
| --- | --- |
| 식별자 | 항목 |
| [SNR#1600](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1600) | 로그인 세션이 유효함에도 로그인 화면이나 "재접속 중입니다" 메시지가 표시되는 문제 해결 |
| [SNR#1625](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1625) | 감사로그 대상 추가 및 감사로그 템플릿 업데이트 |
| [SNR#1753](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1753) | 대시보드 필터 적용/해제 편의성 개선 |
| [SNR#1797](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1797) | 계정 선택 입력 컨트롤 성능 개선 |
| [SNR#1801](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1801) | 정책 메뉴 화면 일관성 개선 |
| [SNR#1804](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1804) | 파서 목록 조회 시 권한 점검 제거 및 스크립트 NullPointerException 수정 |
| [SNR#1824](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1824) | 웹 콘솔 포트를 통한 HTTP POST 로그 수집 지원 |
| [SNR#1905](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1905) | 소명 화면에서 로그 상단 정렬로 변경 및 근거 자료에 조회대상, 데이터유형 필드 제거 |
| [SNR#1912](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1912) | 패턴 그룹 상세 페이지의 패턴 목록 컬럼 너비 개선 |
| [SNR#1916](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1916) | 파이 차트 사용자 색상 지정 기능 추가 |
| [SNR#1918](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1918) | 실시간/배치 탐지 시나리오 설정에서 티켓 담당자를 복수 선택할 수 있도록 변경 |
| [SNR#1938](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1938) | 티켓 작업에 대한 감사 로그 추가 |
| [SNR#1939](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1939) | 로그 화면 검색 필터 세분화 |
| [SNR#1940](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1940) | 네트워크 대역 IP 검색 지원 |
| [SNR#1943](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1943) | 표시 개수 조절 컴포넌트 통일 및 내부 IP 화면에 표시 개수 조절 기능 추가 |
| [SNR#1955](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1955) | 주소 그룹 항목 유지 기간 추가 |
| [SNR#1963](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1963) | 티켓 화면 편의성 및 성능 개선 |
| [SNR#1969](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1969) | 이벤트로부터 티켓 생성 명령어에서 입력 이벤트의 GUID, 시각을 저장하도록 변경 |
| [SNR#2041](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2041) | 동시에 실행되는 배치 시나리오의 개수를 조절하는 시스템 스위치 추가 |
| [SNR#2066](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2066) | remote 쿼리 커맨드 벡터화 |
| [SNR#2074](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2074) | 대형 레코드 수집/쿼리 시 GC 문제 완화 |
| [SNR#2075](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2075) | 파일 수집 시, 사용자 정의 개행문자 지원 |
| [SNR#2077](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2077) | 리눅스 일반 사용자 권한으로 데몬 구동시 NTP 동작 실패하는 문제 해결 |
| [SNR#2078](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2078) | fulltext 커맨드 IPv6 타입 검색 지원 |
| [SNR#2079](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2079) | Syslog 정규식 필터 매칭 병렬화 |
| [SNR#2101](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2101) | GeoIP 데이터베이스 업데이트 반영 |
| [SNR#2110](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2110) | 보안이 강화된 최신 리눅스 배포판(RHEL 9 등)에서 SSH CLI 가 접속되지 않는 문제 해결 |
| [SNR#2107](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2107) | 클라이언트와 서버의 시간 차이 오류 메시지 개선 |
| [SNR#2132](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2132) | geomac 룩업 데이터 업데이트 |
| [SNR#2133](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2133) | 소나 명령어 도움말 및 에러 처리 정리 |
| [SNR#2134](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2134) | event 쿼리 명령어에 duration, order 옵션 추가 |
| [SNR#2139](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2139) | 이중화 로직 개선 |

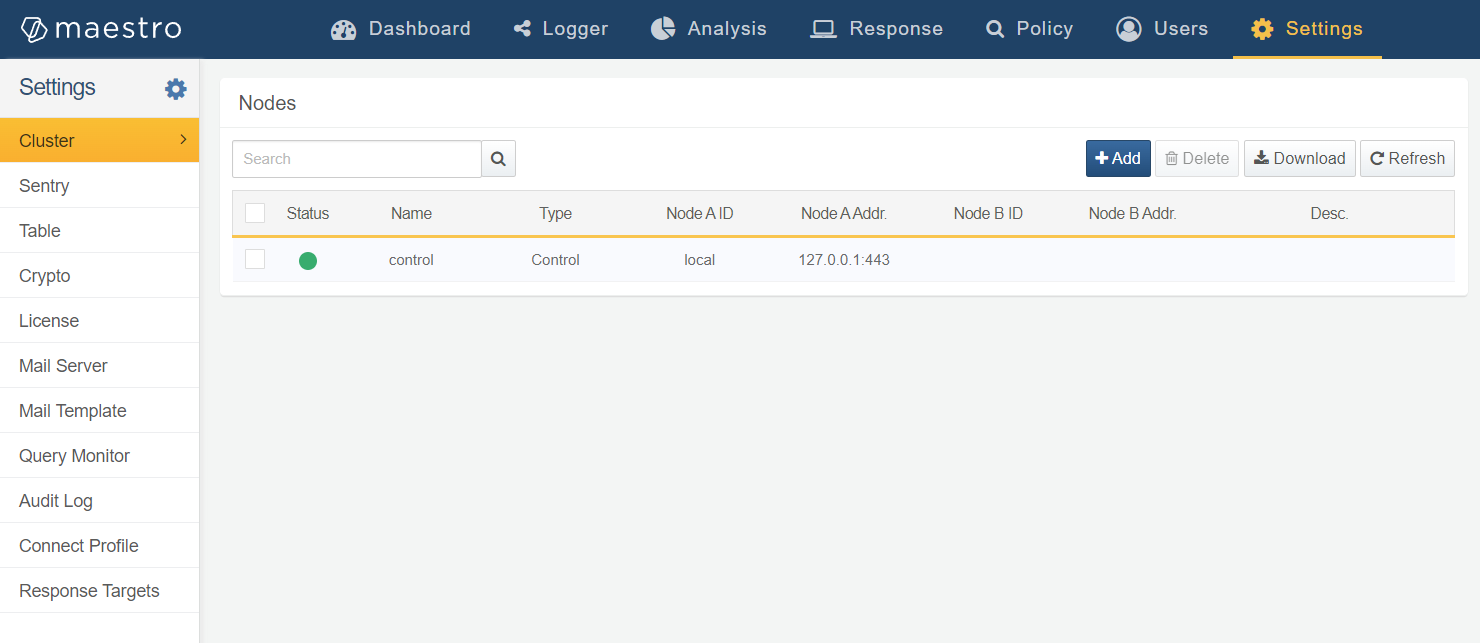
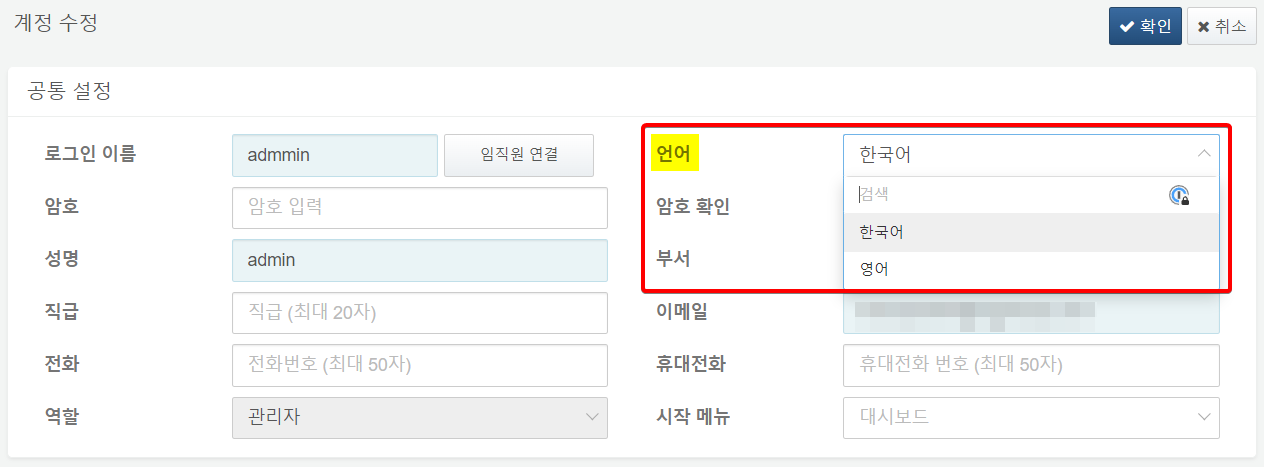
### 버그 해결

|  |  |
| --- | --- |
| 식별자 | 항목 |
| [SNR#1324](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1324) | 검색 창에서 \_, %, \ 문자열이 정상적으로 검색되지 않는 문제 해결 |
| [SNR#1433](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1433) | 목록 화면에서 아무 항목을 선택하지 않아도 삭제 버튼이 활성화되는 문제 해결 |
| [SNR#1465](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1465) | 티켓 분류 삭제 시 삭제되지 않는 티켓 분류도 삭제되었다고 메시지가 표시되는 문제 해결 |
| [SNR#1616](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1616) | 소나 계정이 1000개 이상으로 많으면 계정 목록을 보여주는 화면이 느려지는 문제 해결 |
| [SNR#1719](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1719) | 탐지현황 메뉴에서 분류 항목을 일부 해제했다가 다시 전체 선택하는 경우 그래프 색상이 중복되어 표시되던 문제 해결 |
| [SNR#1763](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1763) | 위젯 생성시 필수 항목을 설정하지 않아도 위젯을 저장할 수 있는 문제 해결 |
| [SNR#1764](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1764) | 대시보드의 첫 위젯을 도킹하면 대시보드 영역의 반이 사용할 수 없는 상태로 변하는 문제 해결 |
| [SNR#1765](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1765) | 대시보드 제목 수정 취소 시 변경에 실패했다는 메세지가 표시되는 문제 해결 |
| [SNR#1769](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1769) | 위젯 설정에서 유효성 검사 메시지가 제대로 표시되지 않는 문제 해결 |
| [SNR#1776](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1776) | 소명 요청 화면에서 임직원 선택 창을 열었다 닫은 후 다시 열면 부서 트리가 제대로 표시되지 않는 문제 해결 |
| [SNR#1818](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1818) | 티켓의 첨부 파일 다운로드가 첫 시도 이후 다시 시도하면 '실패' 라고 표시되는 현상 |
| [SNR#1826](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1826) | 접속 프로파일 수정/삭제 시 기존 접속 프로파일 설정이 없는 경우의 NPE 오류 발생 해결 |
| [SNR#1841](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1841) | 이미지 파일 외에 티켓 첨부 파일 다운로드 시 로그인 화면 출력 되는 문제 |
| [SNR#1843](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1843) | 티켓 본문에 파일 첨부 후 티켓 생성이 안되는 현상 |
| [SNR#1846](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1846) | 첨부파일에 특수문자가 있을 경우 업로드 후 업로드 중 텍스트가 변경되지 않음 |
| [SNR#1851](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1851) | 종속 변수 수동 추가시 범례 순서가 반영되지 않는 현상 |
| [SNR#1882](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1882) | 쿼리 위젯 이름 50자 초과 입력 시 validator 동작하지 않고 생성 실패하는 현상 |
| [SNR#1883](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1883) | 쿼리 화면에서 테이블 트리 필터/체크 후, 테이블 선택된 항목이 해제되지 않는 오류 해결 |
| [SNR#1913](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1913) | 마에스트로 티켓 생성 명령어의 중요도 설정이 되지 않는 문제 해결 |
| [SNR#1936](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1936) | 플레이북 디자이너에서 태스크 정렬 기능이 동작하지 않는 문제 해결 |
| [SNR#1937](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1937) | 머신러닝 모델에 사용 중인 학습 데이터셋 삭제 시 오류 메시지 등 보완 |
| [SNR#1981](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1981) | 탐지 현황 팝업에서 info 버튼 클릭 시 자세한 정보 보기 내용 잘림 |
| [SNR#1999](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR1999) | 시나리오에서 중복 이벤트 제거를 설정한 경우, 티켓 삭제 및 완료 처리 시 NPE 오류 발생 해결 |
| [SNR#2022](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2022) | 티켓 축약 0초 설정 시 100ms 범위 내 생성된 티켓이 축약되는 문제 |
| [SNR#2023](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2023) | 보고서 서식 다운로드시 현재 페이지만 다운로드 되는 오류 |
| [SNR#2031](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2031) | 수집기 선택 트리에서 테이블 조회 권한이 없는 수집기가 표시되는 문제 해결 |
| [SNR#2043](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2043) | 사용자 정의 변수를 사용하는 대시보드를 공유하였을 때, 사용자 계정에서 입력 컨트롤을 사용할 수 없는 문제 해결 |
| [SNR#2050](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2050) | table, fulltext 커맨드의 테이블 중복 지정에 따른 결과 반복 출력되는 문제 해결 |
| [SNR#2062](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2062) | 티켓 정오탐 및 사고 여부 변경 권한이 클러스터 관리자에게만 부여된 문제 해결 |
| [SNR#2064](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2064) | 분석 노드에서 테이블 삭제 시 수집 노드에서 테이블 데이터 파일이 삭제되지 않고 남아있는 문제 해결 |
| [SNR#2073](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2073) | fulltext 쿼리 명령어의 중첩된 부등호 연산 정합성 문제 해결 |
| [SNR#2085](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2085) | ldapsearch 쿼리 명령어에서 1,000건 결과 제한으로 실패하는 오류 해결 |
| [SNR#2093](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2093) | parse 커맨드의 overlay 옵션이 누락되는 현상 해결 |
| [SNR#2094](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2094) | 센트리 Linux Account Watcher 수집기 영문으로 표시 |
| [SNR#2095](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2095) | SNMP 수집기 설정에 잘못된 oid 필드 매핑 값을 입력했을 때 오류 처리 추가 |
| [SNR#2103](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2103) | 특정 쿼리 커맨드에서 쿼리에 매개변수 사용 불가능한 문제 해결 |
| [SNR#2104](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2104) | 인덱스 동시 접근 시 인덱스 토크나이저가 누수되는 문제 해결 |
| [SNR#2108](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2108) | SNMP 수집 버그 수정 |
| [SNR#2127](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2127) | 쿼리 종료 대기로 인한 셧다운 hang |
| [SNR#2145](https://docs.logpresso.com/ko/sonar/4.0/issues/SNR2145) | 라이선스 주입 시 버전 4 인식 실패 |

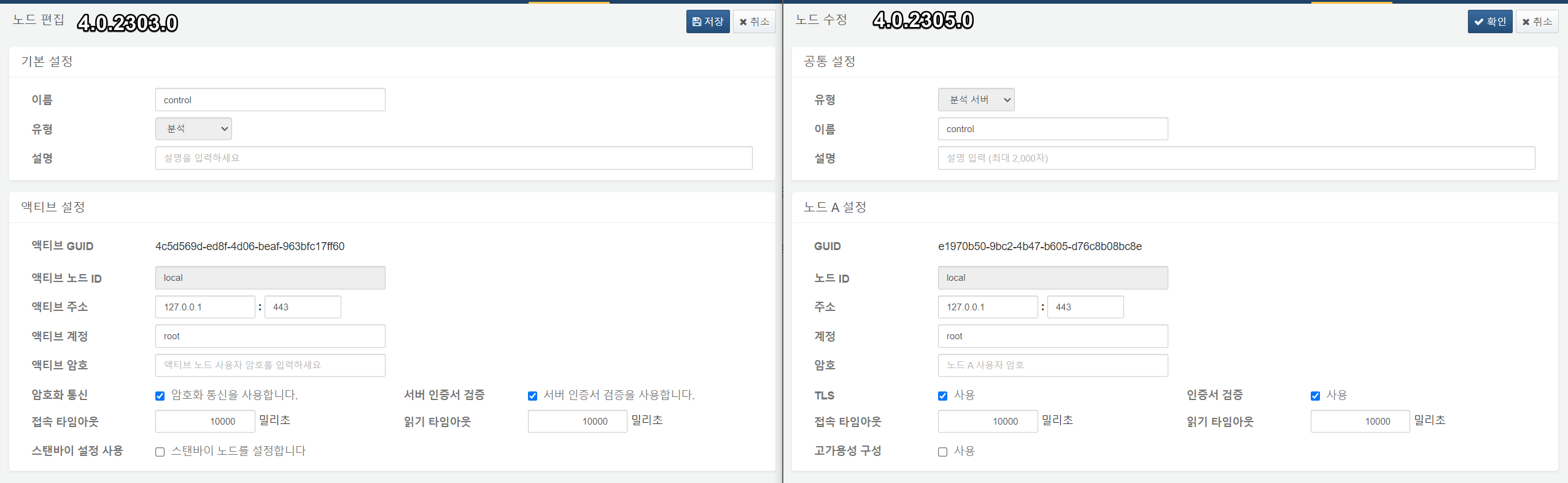
### 상세 내역

#### SNR#1612 다국어 로케일 지원

영어 로케일 지원이 추가되었습니다. 계정 생성/수정 메뉴에서 언어를 선택할 수 있는 항목이 추가되었으며 영어를 선택할 경우 영어 로케일로 표시됩니다.



국문 로케일도 좀 더 자연스러운 표현으로 개선되었습니다.



#### SNR#1761 REST API 지원

113종의 로그프레소 소나 REST API를 지원합니다. 각 REST API에 대한 요청 및 응답 명세는 [REST API 레퍼런스](https://docs.logpresso.com/ko/sonar/4.0/api)를 참고하세요.

https://hostname/api/ 주소로 접속하면 REST API 테스트 페이지를 이용할 수 있습니다. REST API 테스트 페이지 인증은 웹 콘솔 로그인 계정과 동일합니다.



자바스크립트에서 직접 로그프레소 REST API를 호출할 수 있도록 허용하려면 로그프레소 시스템 스위치에 다음 항목을 추가하세요:

-Dlogpresso.httpd.cors=enabled-Daraqne.httpd.options\_method=enabled

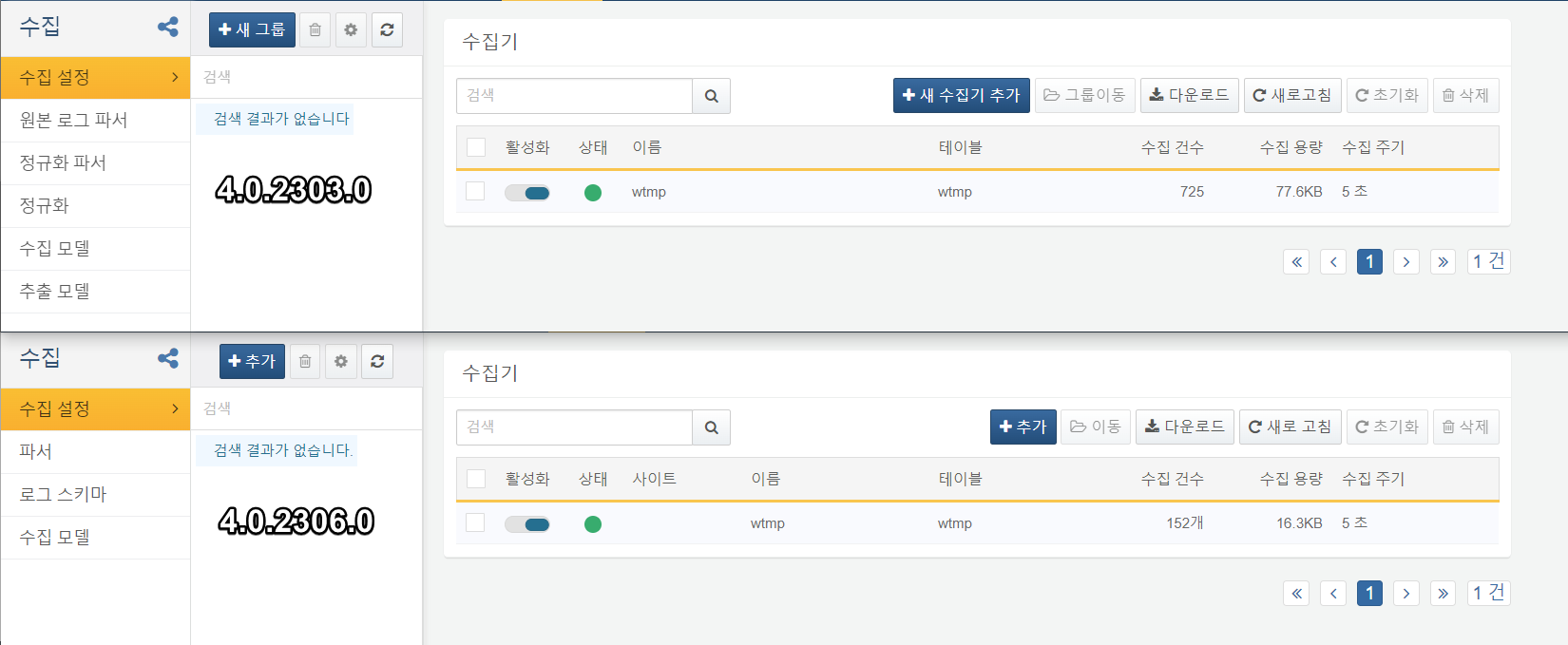
**REST API 기능 목록**

|  |  |  |
| --- | --- | --- |
| 번호 | 분류 | 항목 |
| 1 | 쿼리 | 쿼리 |
| 2 | 쿼리 | 쿼리 상태 조회 |
| 3 | 쿼리 | 커서 생성 |
| 4 | 쿼리 | 커서 조회 |
| 5 | 쿼리 | 커서 삭제 |
| 6 | 계정 | 암호 인증 |
| 7 | 계정 | 계정 목록 조회 |
| 8 | 계정 | 계정 조회 |
| 9 | 계정 | 계정 생성 |
| 10 | 계정 | 계정 수정 |
| 11 | 계정 | 계정 일괄 삭제 |
| 12 | 계정 그룹 | 계정 그룹 목록 조회 |
| 13 | 계정 그룹 | 계정 그룹 조회 |
| 14 | 계정 그룹 | 계정 그룹 생성 |
| 15 | 계정 그룹 | 계정 그룹 수정 |
| 16 | 게정 그룹 | 계정 그룹 일괄 삭제 |
| 17 | 접속 프로파일 | 접속 프로파일 유형 목록 조회 |
| 18 | 접속 프로파일 | 접속 프로파일 설정 명세 조회 |
| 19 | 접속 프로파일 | 접속 프로파일 목록 조회 |
| 20 | 접속 프로파일 | 접속 프로파일 조회 |
| 21 | 접속 프로파일 | 접속 프로파일 생성 |
| 22 | 접속 프로파일 | 접속 프로파일 수정 |
| 23 | 접속 프로파일 | 접속 프로파일 삭제 |
| 24 | 접속 프로파일 | SSH 공개 키 조회 |
| 25 | 접속 프로파일 | SSH 공개 키 재생성 |
| 26 | 파서 | 파서 유형 목록 조회 |
| 27 | 파서 | 파서 유형 조회 |
| 28 | 파서 | 파서 목록 조회 |
| 29 | 파서 | 파서 조회 |
| 30 | 파서 | 파서 생성 |
| 31 | 파서 | 파서 수정 |
| 32 | 파서 | 파서 일괄 삭제 |
| 33 | 파서 | 파서 테스트 |
| 34 | 로그 스키마 | 로그 스키마 목록 조회 |
| 35 | 로그 스키마 | 로그 스키마 조회 |
| 36 | 로그 스키마 | 로그 스키마 생성 |
| 37 | 로그 스키마 | 로그 스키마 수정 |
| 38 | 로그 스키마 | 로그 스키마 일괄 삭제 |
| 39 | 주소 그룹 | 주소 그룹 목록 조회 |
| 40 | 주소 그룹 | 주소 그룹 조회 |
| 41 | 주소 그룹 | 주소 그룹 생성 |
| 42 | 주소 그룹 | 주소 그룹 수정 |
| 43 | 주소 그룹 | 주소 그룹 일괄 삭제 |
| 44 | 주소 그룹 | 주소 객체 목록 조회 |
| 45 | 주소 그룹 | 주소 객체 생성 |
| 46 | 주소 그룹 | 주소 객체 일괄 삭제 |
| 47 | 네트워크 대역 그룹 | 네트워크 대역 그룹 목록 조회 |
| 48 | 네트워크 대역 그룹 | 네트워크 대역 그룹 조회 |
| 49 | 네트워크 대역 그룹 | 네트워크 대역 그룹 생성 |
| 50 | 네트워크 대역 그룹 | 네트워크 대역 그룹 수정 |
| 51 | 네트워크 대역 그룹 | 네트워크 대역 그룹 일괄 삭제 |
| 52 | 네트워크 대역 그룹 | 네트워크 대역 목록 조회 |
| 53 | 네트워크 대역 그룹 | 네트워크 대역 생성 |
| 54 | 네트워크 대역 그룹 | 네트워크 대역 수정 |
| 55 | 네트워크 대역 그룹 | 네트워크 대역 일괄 삭제 |
| 56 | 패턴 그룹 | 패턴 그룹 목록 조회 |
| 57 | 패턴 그룹 | 패턴 그룹 조회 |
| 58 | 패턴 그룹 | 패턴 그룹 생성 |
| 59 | 패턴 그룹 | 패턴 그룹 수정 |
| 60 | 패턴 그룹 | 패턴 그룹 일괄 삭제 |
| 61 | 패턴 그룹 | 패턴 목록 조회 |
| 62 | 패턴 그룹 | 패턴 생성 |
| 63 | 패턴 그룹 | 패턴 수정 |
| 64 | 패턴 그룹 | 패턴 일괄 삭제 |
| 65 | 테이블 | 테이블 목록 조회 |
| 66 | 테이블 | 테이블 조회 |
| 67 | 테이블 | 테이블 생성 |
| 68 | 테이블 | 테이블 삭제 |
| 69 | 테이블 | 테이블 파티션 삭제 |
| 70 | 테이블 | 테이블 보관주기 설정 |
| 71 | 실시간 탐지 시나리오 | 실시간 탐지 시나리오 목록 조회 |
| 72 | 실시간 탐지 시나리오 | 실시간 탐지 시나리오 조회 |
| 73 | 실시간 탐지 시나리오 | 실시간 탐지 시나리오 생성 |
| 74 | 실시간 탐지 시나리오 | 실시간 탐지 시나리오 수정 |
| 75 | 실시간 탐지 시나리오 | 실시간 탐지 시나리오 삭제 |
| 76 | 실시간 탐지 시나리오 | 실시간 탐지 시나리오 활성화 |
| 77 | 실시간 탐지 시나리오 | 실시간 탐지 시나리오 비활성화 |
| 78 | 실시간 탐지 시나리오 | 실시간 탐지 명령어 템플릿 목록 조회 |
| 79 | 실시간 탐지 시나리오 | 실시간 탐지 명령어 템플릿 조회 |
| 80 | 배치 탐지 시나리오 | 배치 탐지 시나리오 목록 조회 |
| 81 | 배치 탐지 시나리오 | 배치 탐지 시나리오 조회 |
| 82 | 배치 탐지 시나리오 | 배치 탐지 시나리오 생성 |
| 83 | 배치 탐지 시나리오 | 배치 탐지 시나리오 수정 |
| 84 | 배치 탐지 시나리오 | 배치 탐지 시나리오 삭제 |
| 85 | 배치 탐지 시나리오 | 배치 탐지 시나리오 실행 |
| 86 | 배치 탐지 시나리오 | 배치 탐지 시나리오 활성화 |
| 87 | 배치 탐지 시나리오 | 배치 탐지 시나리오 비활성화 |
| 88 | 티켓 | 티켓 목록 조회 |
| 89 | 티켓 | 티켓 조회 |
| 90 | 티켓 | 티켓 생성 |
| 91 | 티켓 | 티켓 수정 |
| 92 | 티켓 | 티켓 일괄 삭제 |
| 93 | 티켓 | 티켓 중요도 수정 |
| 94 | 티켓 | 티켓 제목 수정 |
| 95 | 티켓 | 티켓 정오탐 수정 |
| 96 | 티켓 | 티켓 사고 여부 수정 |
| 97 | 티켓 | 티켓 담당자 할당 |
| 98 | 티켓 | 티켓 담당자 목록 조회 |
| 99 | 티켓 | 티켓 담당자 상태 변경 |
| 100 | 티켓 | 티켓 완료 처리 |
| 101 | 티켓 | 티켓 다시 열기 |
| 102 | 티켓 | 티켓 결재 요청 |
| 103 | 티켓 | 티켓 결재 승인 |
| 104 | 티켓 | 티켓 결재 반려 |
| 105 | 티켓 | 티켓 첨부 파일 목록 조회 |
| 106 | 티켓 | 티켓 첨부 파일 삭제 |
| 107 | 티켓 | 티켓 메모 목록 조회 |
| 108 | 티켓 | 티켓 메모 추가 |
| 109 | 티켓 | 티켓 메모 수정 |
| 110 | 티켓 | 티켓 메모 삭제 |
| 111 | 소명 템플릿 | 소명 템플릿 목록 조회 |
| 112 | 소명 템플릿 | 소명 템플릿 조회 |
| 113 | 소명 템플릿 | 소명 템플릿 설정 |

#### SNR#2028 파서 및 수집 모델 UI 간소화

파서 및 수집 모델 UI를 간소화하여 수집 설정 구축 프로세스를 개선했습니다. 원본 로그 파서와 정규화 파서는 파서로 통합되었고, 수집 모델과 추출 모델은 수집 모델로 통합되었습니다. 자세한 변경 사항은 다음과 같습니다.

* 원본 로그 파서와 정규화 파서가 파서로 통합되면서 파서에 정규화 기능이 제외되고, 추출모델이 수집모델에 통합되면서 수집모델에서 정규화 규칙을 설정하게 되었습니다.
* 수집 메뉴 화면도 기존에 수집 설정, 원본 로그 파서, 정규화 파서, 정규화, 수집 모델, 추출 모델 탭이 수집 설정, 파서, 로그 스키마, 수집 모델 탭으로 간소화되었습니다.
* 수집 설정에 필터 설정 항목이 추가되었습니다.
* "정규화"가 "로그 스키마"라는 이름으로 용어가 변경되었습니다.



변경된 수집 메뉴에서 신규 수집 설정을 추가하려면 다음과 같이 진행하면 됩니다.

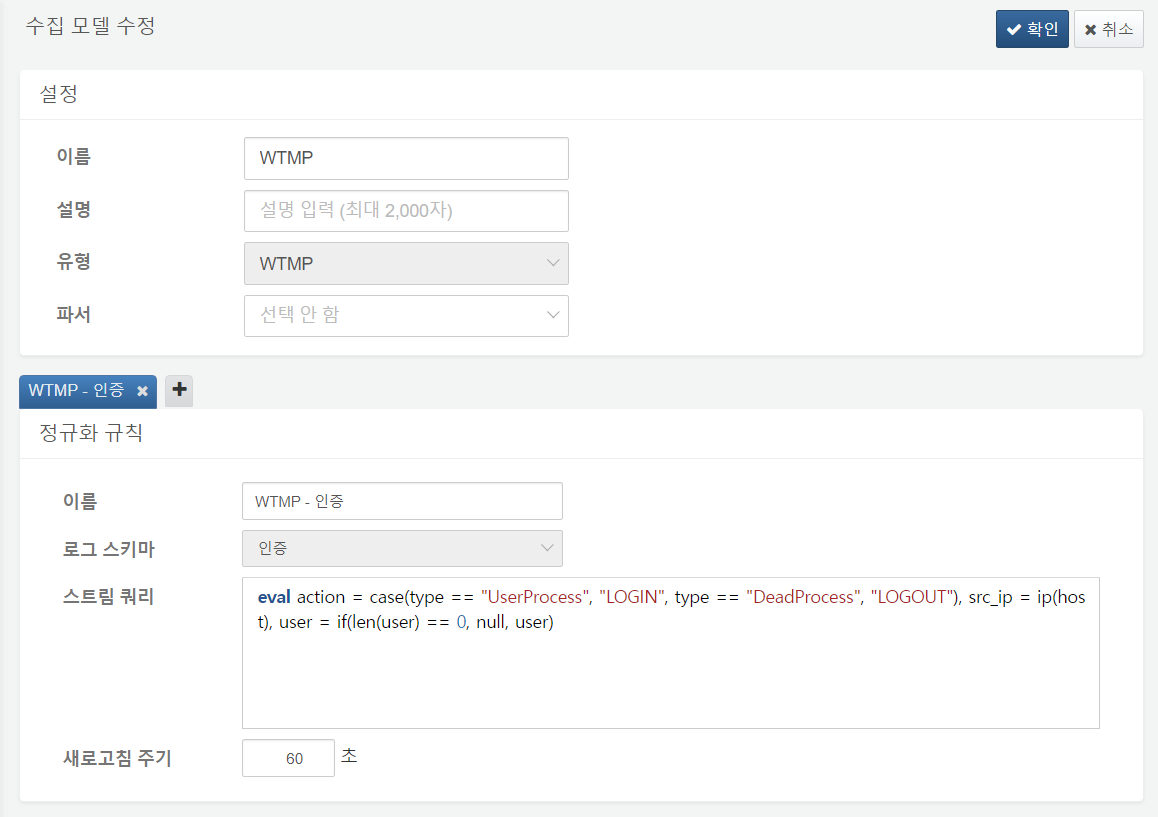
로그 스키마 설정

* 기존 버전의 정규화와 동일한 방법으로 로그 스키마 필드들을 정의해주시면 됩니다.

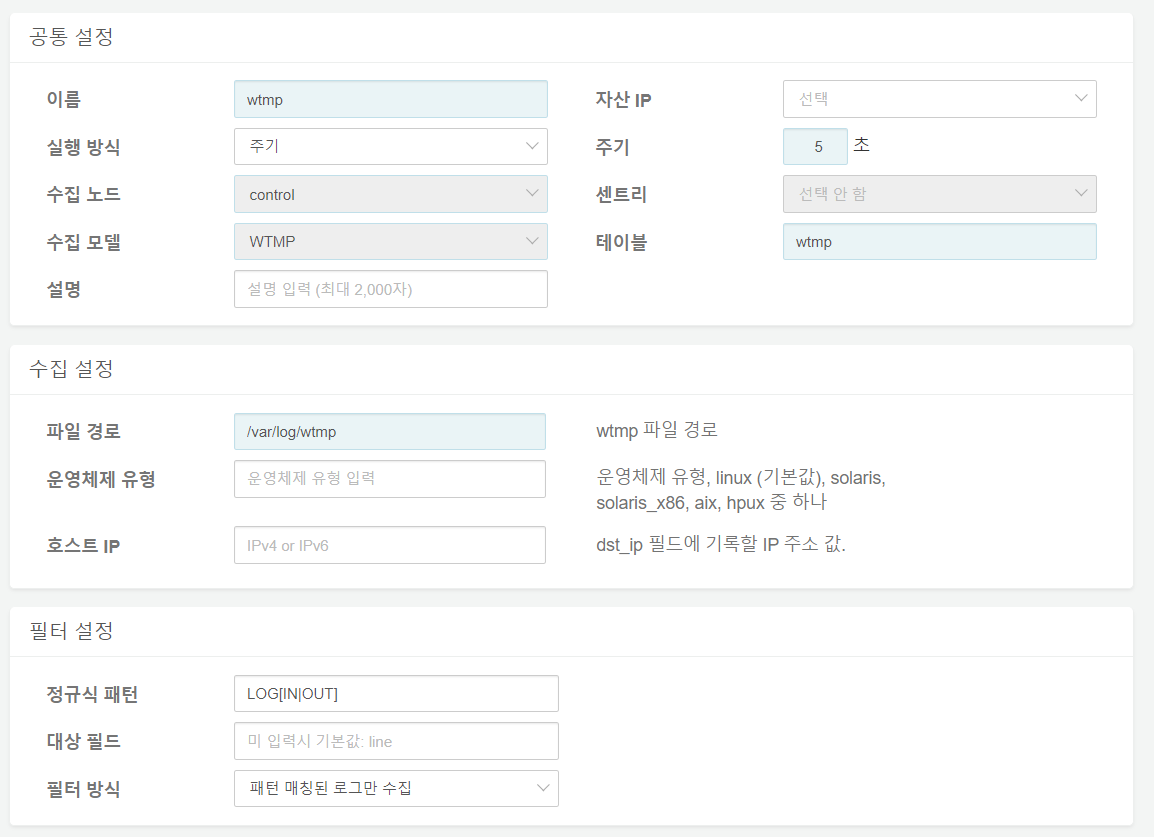
파서 설정

* 기존 버전의 원본 로그 파서와 동일한 방법으로 설정하시면 됩니다.

수집 모델 설정

* 기존 버전의 수집 모델과 동일하게 수집 유형 및 파서를 선택합니다. 그 후 정규화 규칙을 설정하는 과정은 기존 버전에서 추출 모델을 설정할 때와 유사합니다. 수집된 로그에 적용할 스트림 쿼리를 입력하고, 로그 조회시 적용할 로그 스키마를 설정합니다. 하나의 수집 모델에 여러 개의 정규화 규칙을 설정할 수 있습니다.

수집기 설정

* 기존 버전과 동일하게 공통 설정을 입력하고 수집 모델을 선택하여 수집 설정을 입력합니다. 입력받는 로그 중 특정 로그만 수집하거나 제외하고 싶은 경우 필터 설정을 입력합니다. 대상 필드에 정규식 패턴을 매칭하여 필터 방식에 따라 해당 로그를 수집하거나 제외합니다.

패치 시 기존 설정은 다음과 같이 반영됩니다.

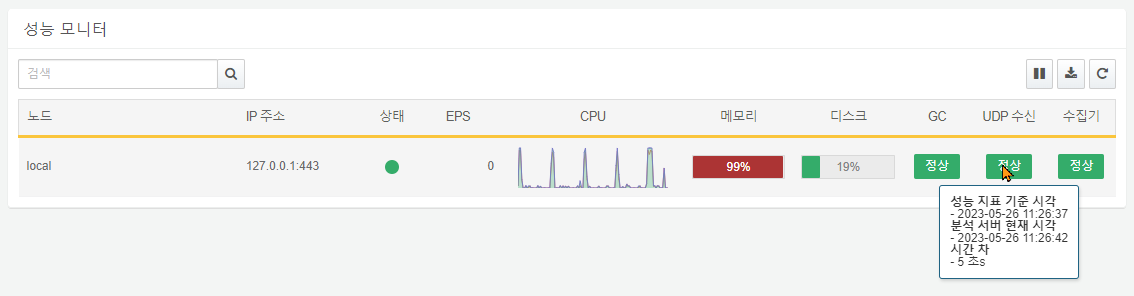
* 패치 전 생성한 원본 로그 파서는 기존 설정을 유지합니다.
* 패치 전 생성한 정규화 파서는 로그 스키마를 포함한 기존 설정을 유지한 채 이관됩니다. 다만 신규 파서 생성 시 로그 스키마(구 정규화)를 적용할 수 없습니다.
* 패치 전 생성한 수집 모델은 기존 설정을 유지한 채 이관됩니다.
* 패치 전 생성한 추출 모델은 로그 스키마와 스트림 쿼리 설정이 유지된 채로 연결된 수집 모델에 정규화 규칙으로 포함됩니다.

#### SNR#2029 성능 모니터 메뉴 추가

연결된 모든 노드에 대해 각 노드 별 성능 지표를 확인할 수 있는 "성능 모니터" 메뉴가 추가되었습니다. 성능 모니터 메뉴에서 각 노드 장비가 과부하 상태나 디스크 부족 상태는 아닌지, 수집은 정상적으로 이루어지고 있는지, 네트워크 연결은 정상인지, 데이터 수신 단에서 유실이 발생하고 있지는 않는지 확인할 수 있습니다.

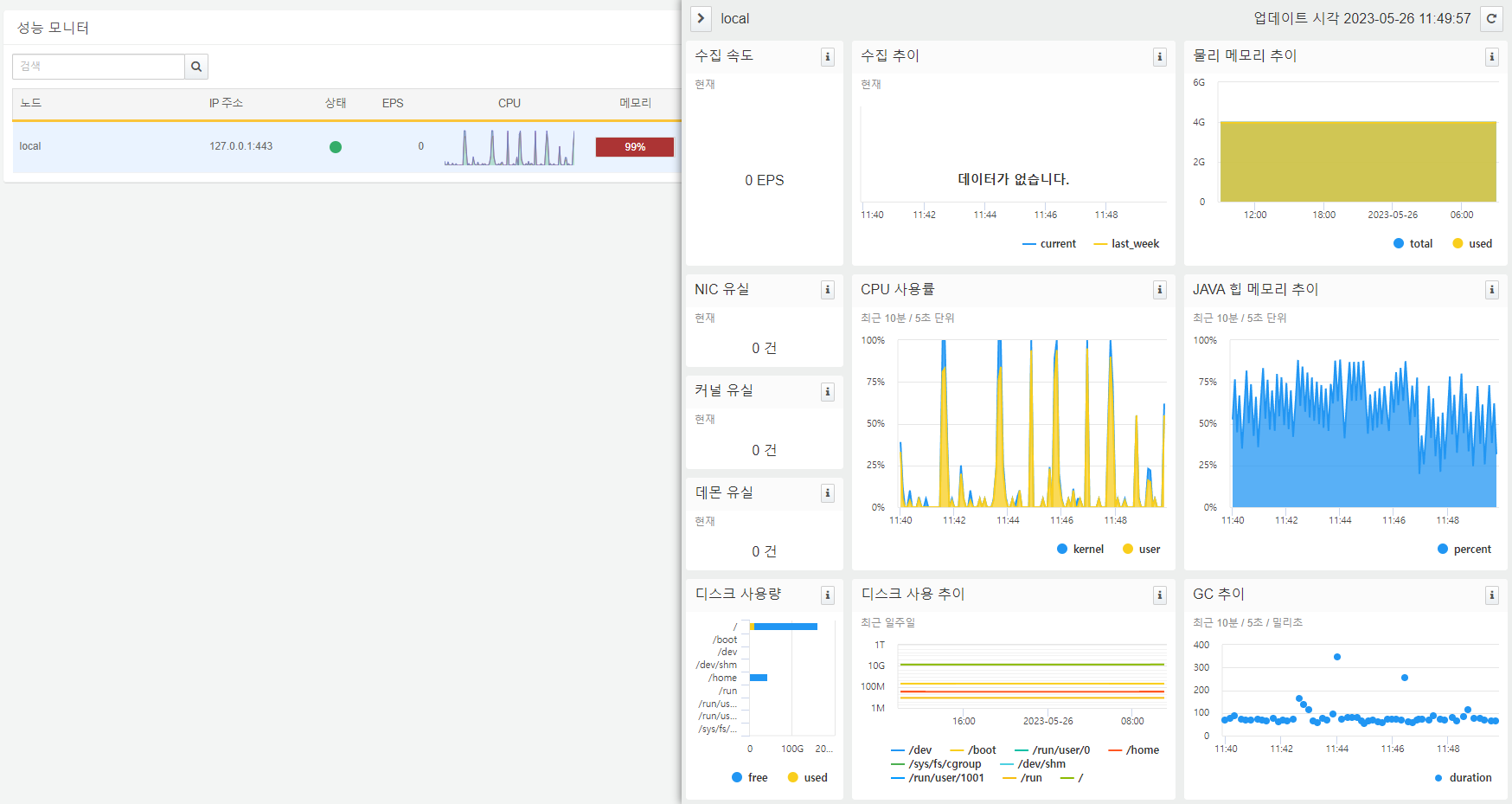
성능 모니터 메뉴에 들어가면 연결된 모든 노드에 대한 성능 추이가 목록 형태로 간략히 표시됩니다. 표시되는 항목은 다음과 같습니다.

* 노드 이름
* 노드 IP 주소
* 노드 활성화 상태
* 노드 수집 속도 (EPS)
* 노드 CPU 사용률
* 노드 메모리 사용률
* 노드 디스크 사용률
* 노드 GC 상태
* 노드 UDP 수신 상태



특정 노드를 클릭하면 사이드 패널로 해당 노드의 상세 성능 추이가 표시됩니다. 표시되는 항목은 다음과 같습니다.

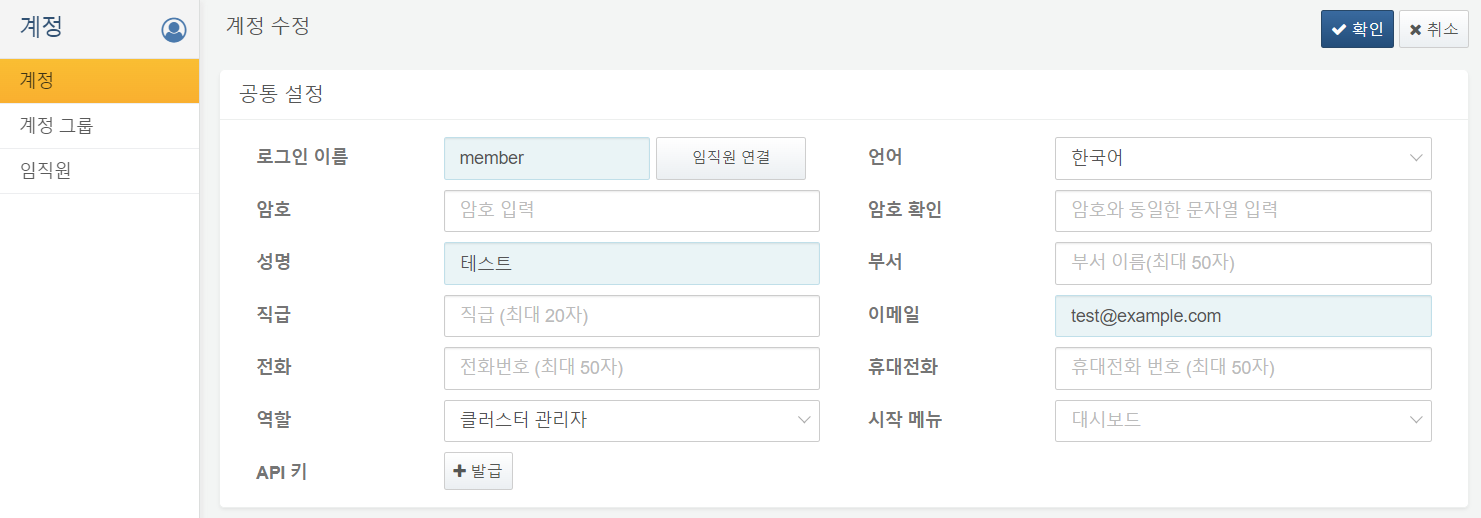
* 수집 속도
* 수집 추이
* 물리 메모리 추이
* NIC 유실
* 커널 유실
* 데몬 유실
* CPU 사용률
* JAVA 힙 메모리 추이
* 디스크 사용량
* 디스크 사용 추이
* GC 추이



#### SNR#2038 멀티 테넌트 기능 파기

멀티 테넌트 기능을 사용하고 있는 경우, 패치 전 기존 데이터베이스 백업 및 테넌트 이관 작업을 진행해주시길 바랍니다.

로그프레소 소나에서 여러 회사를 관리할 수 있는 멀티 테넌트 기능을 파기하였습니다. 계정 메뉴에서 회사 탭이 사라졌고 계정, 임직원 상세 정보에 회사 항목이 삭제되었습니다.

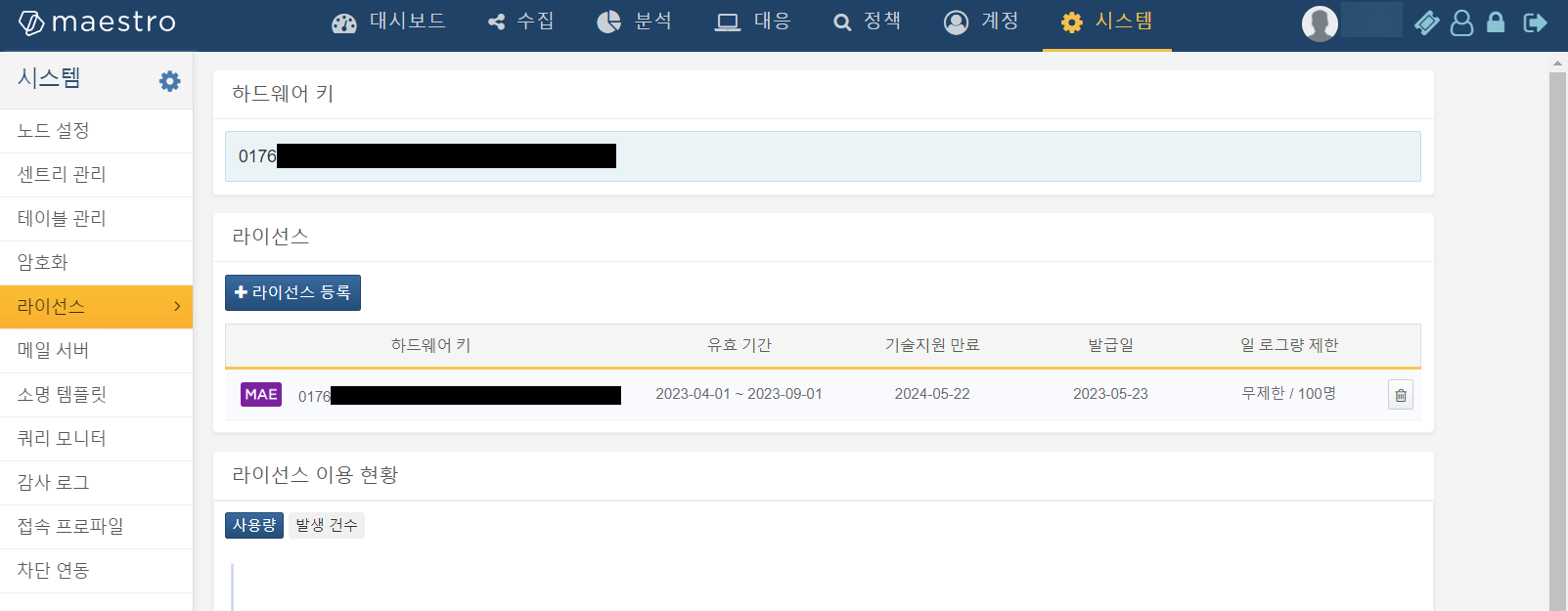


#### SNR#2044 사이트, 호스트명, 자산 태깅(다수의 고객사 관제 지원)

#### SNR#2045 로그프레소 제품 단일 패키지화 및 라이선스 체계 변경

기존에 Standard(STD), Enterprise(ENT), Sonar(SNR), Maestro(MAE)로 나뉘던 로그프레소 제품군이 Sonar Light, Sonar, Maestro 로 구분되도록 변경되었습니다. STD, ENT 제품은 모두 Sonar Light 제품군으로 통합되었습니다.

패키징 또한 각각 개별 패키지 파일이 존재하던 방식에서, 단일 패키지 구조로 변경되었습니다. 어느 라이선스를 설치하냐에 따라 제공되는 제품의 기능이 달라집니다.

* STD 라이선스 적용 시 Sonar Light 메뉴만 표시
* MAE 라이선스 적용 시 Maestro 메뉴 표시

이에 따라 서버 패키지를 다시 설치하지 않더라도 라이선스 업그레이드 시 즉시 추가된 기능을 사용할 수 있습니다.

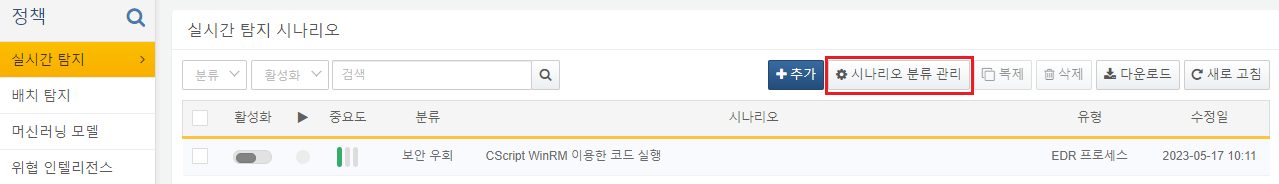
#### SNR#2055 스토리지 생명주기 지원

#### SNR#2068 단일 노드 구성에 대해 SQLite 백엔드 지원

노드 이중화를 사용하지 않고 별도의 수집 노드 없이 단일 노드 구성으로 로그프레소를 구축하는 경우, MariaDB 대신 SQLite를 사용할 수 있는 옵션을 지원합니다.최초 설치 시 시스템 스위치에 logpresso.sonar.sqlite=true 를 추가하면 로그프레소가 SQLite 기반으로 동작합니다.

#### SNR#1773 시나리오 분류 관리 기능 추가 및 소명 분류 관리 화면을 팝업으로 변경

실시간/배치 탐지 시나리오 목록에 시나리오 분류 관리 기능이 추가되었습니다.

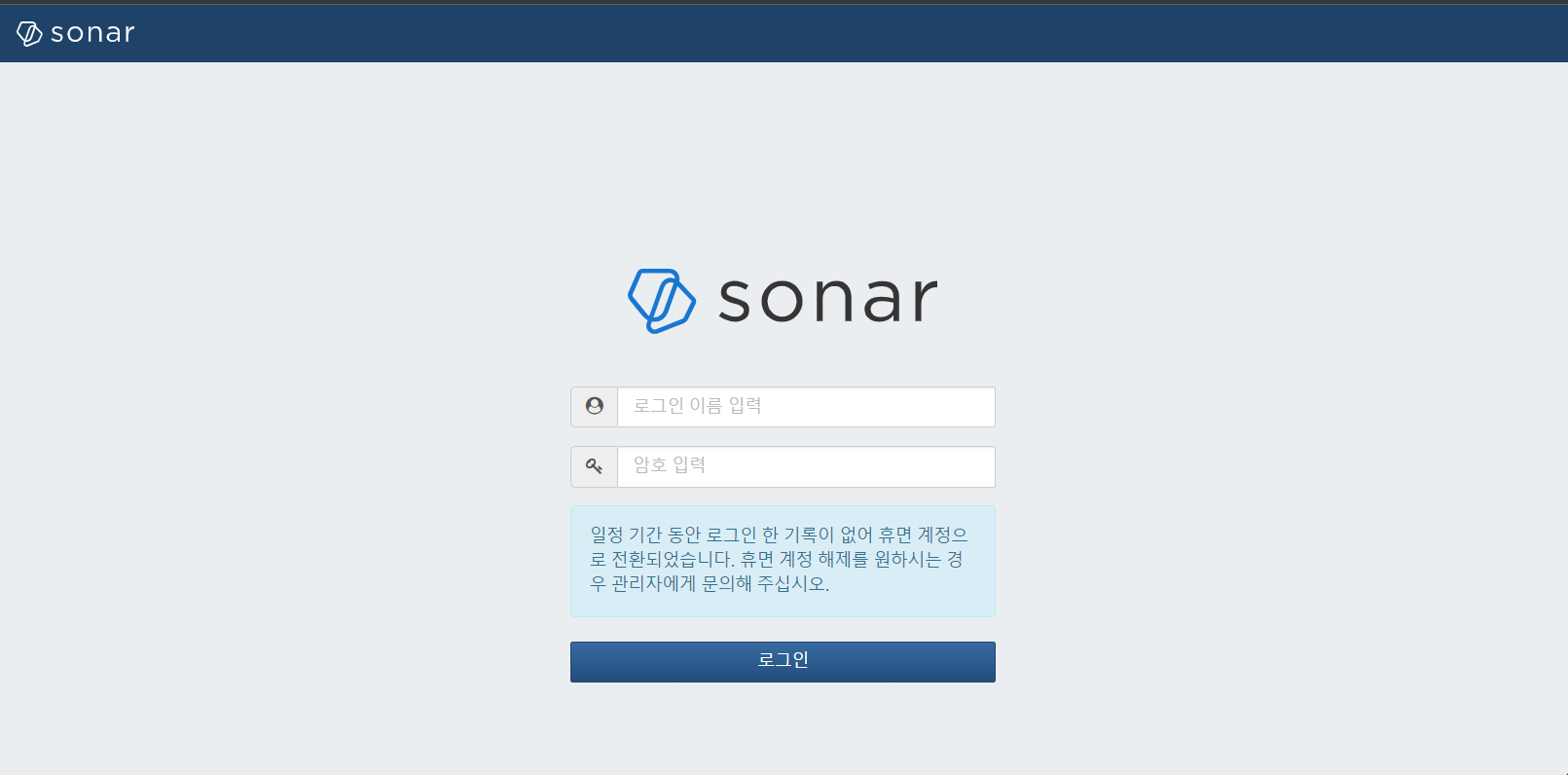
* 실시간/배치 탐지 시나리오 목록
* 시나리오 분류 관리 팝업

소명 분류 관리 화면은 화면 전환에서 시나리오 분류 관리와 동일하게 팝업으로 변경하였습니다.

#### SNR#1782 휴면 계정 전환 기능 추가

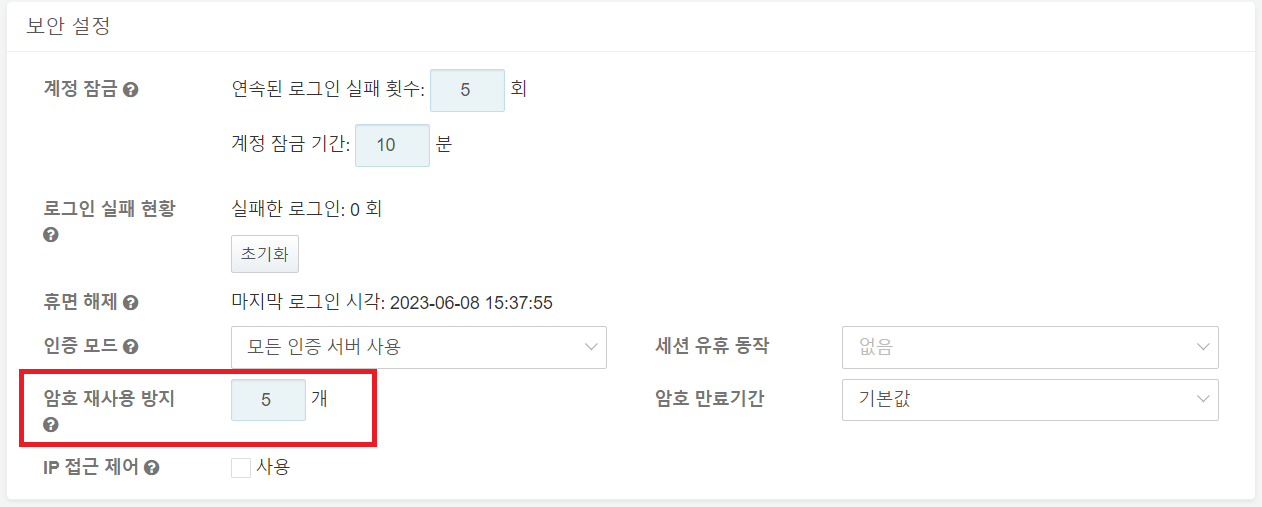
일정 기간 동안 로그인하지 않은 계정에 대해 휴면 전환 정책을 적용할 수 있도록 기능이 추가되었습니다.휴면 계정 전환 정책을 설정한 경우(예시는 180일)에 기능이 활성화됩니다. 기본 정책은 휴면 계정 전환 기능 비활성화입니다.

logpresso> sonar.setGlobalOption inactive\_account\_period 180

* 휴면 계정 전환 기준: 마지막 로그인 시각(없는 경우, 계정 생성일)이 설정한 정책 일수보다 오래되면 휴면 계정으로 전환
* 휴면 계정으로 로그인 시 안내 메시지 화면
* 휴면 해제 기능: 관리자 이상 계정에서 휴면 계정에 대해 해제 기능 활성화됨

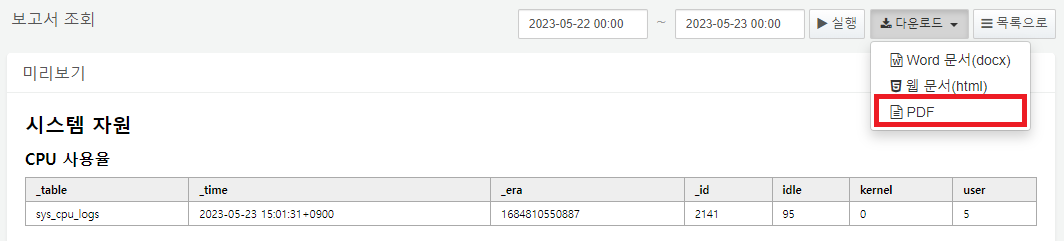
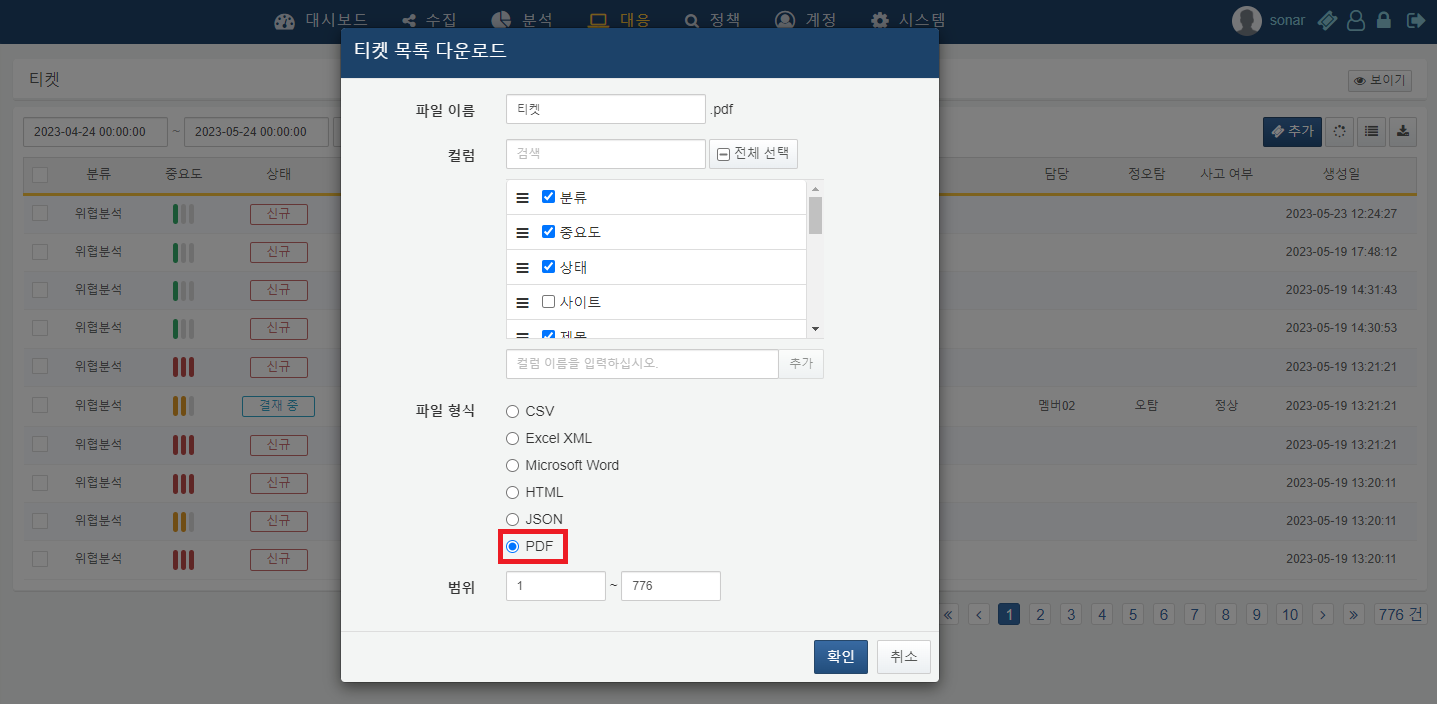
#### SNR#1783 계정 최소 암호 길이 및 암호 재사용 방지 정책 설정 기능 추가

로그인 계정의 최소 암호 길이 및 암호 재사용 방지 정책을 설정할 수 있는 기능이 추가되었습니다.

* 로그인 계정 최소 암호 길이 정책 설정(예시 10자): 모든 계정에 전역적으로 설정
* sonar.setGlobalOption min\_password\_len 10
* 설정 허용값 범위: 3자 이상 (암호 복잡도 충족을 위한 최소 길이)
* 암호 복잡도: 영문, 숫자, 특수문자, 3자 이상의 연속된 영문(숫자)가 아닌 조합
* 정책 미설정 시 기본값: 9자
* 로그인 계정 암호 재사용 방지 정책 설정: 관리자 이상 계정에서 각 사용자의 정책을 설정
* 설정 허용값 범위: 0 ~ 23개
* 정책 미설정 시 기본값: 1개

#### SNR#1947 보고서 및 다운로드 파일 형식에 PDF 포맷 추가

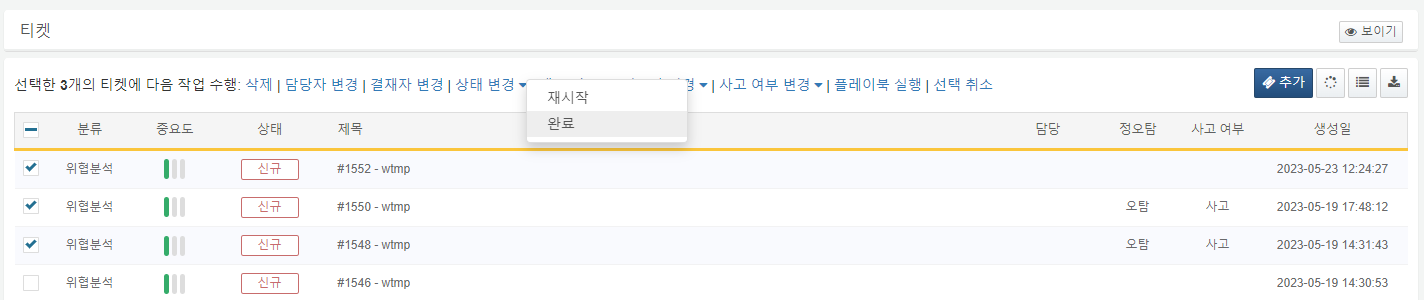
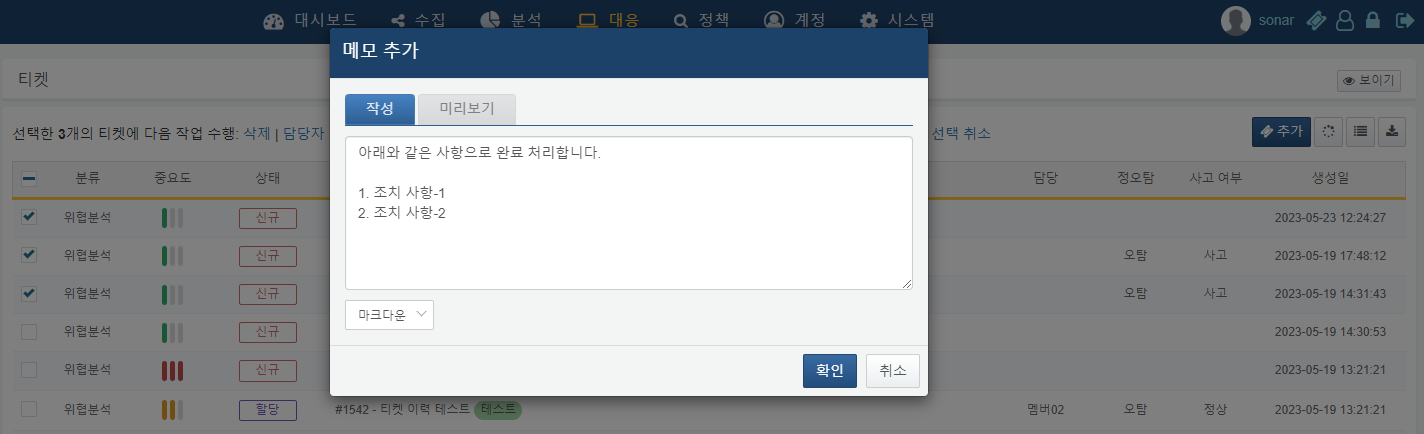
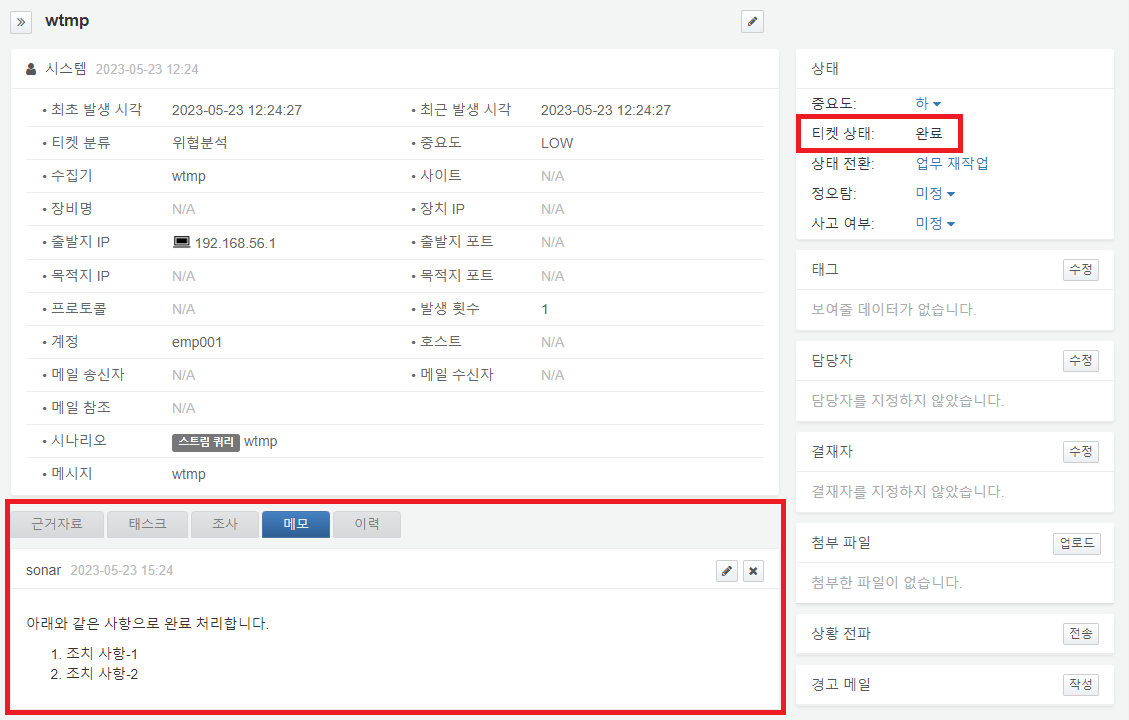
보고서 및 각 화면 다운로드 파일 형식에 PDF 포맷을 추가하였습니다.

* 보고서 다운로드
* 화면 다운로드

#### SNR#1962 티켓 일괄 작업 시 메모 입력 기능 추가

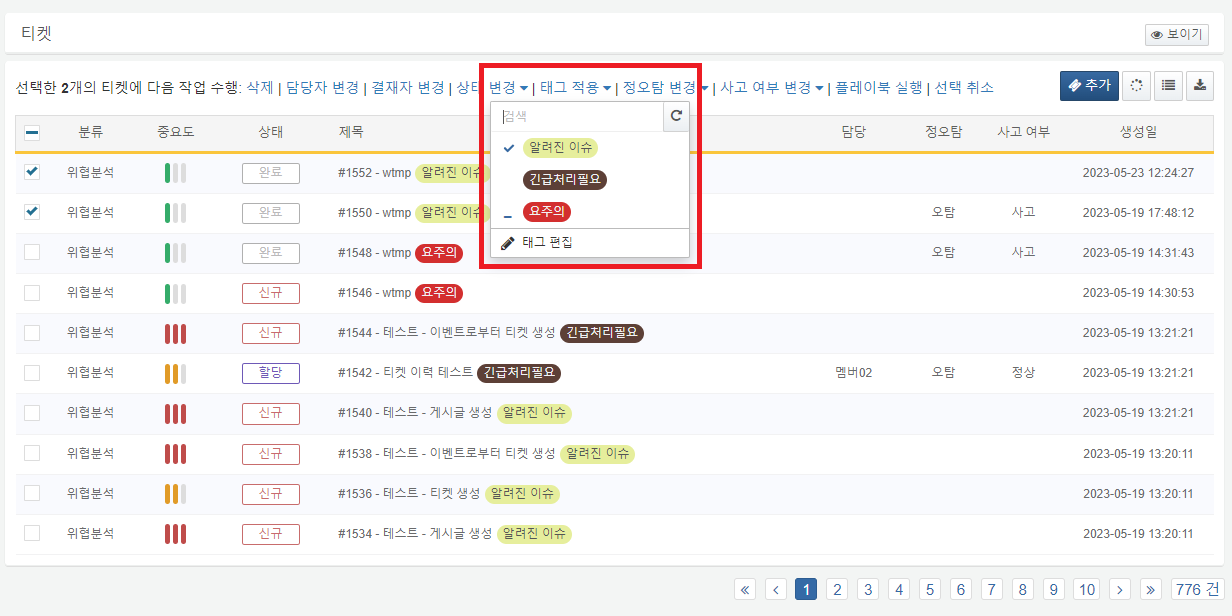
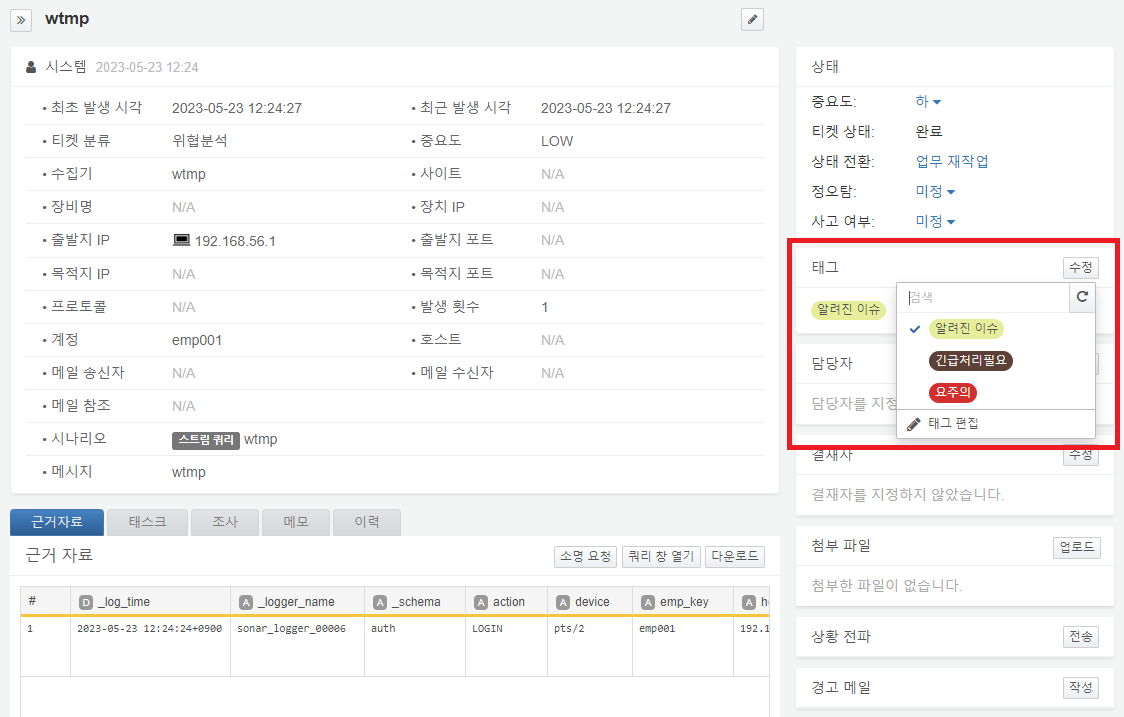
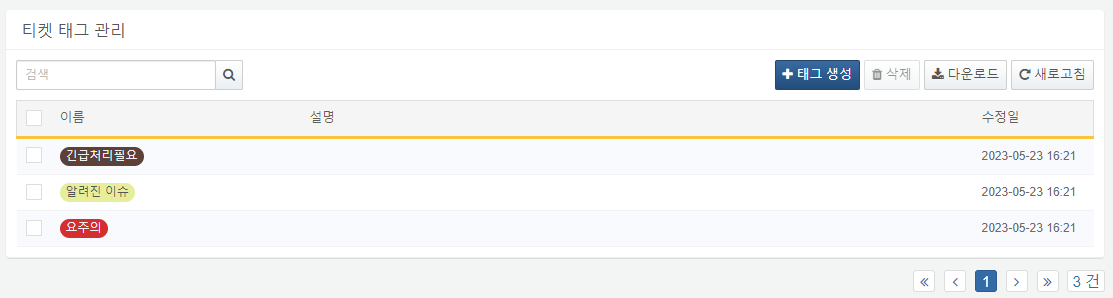
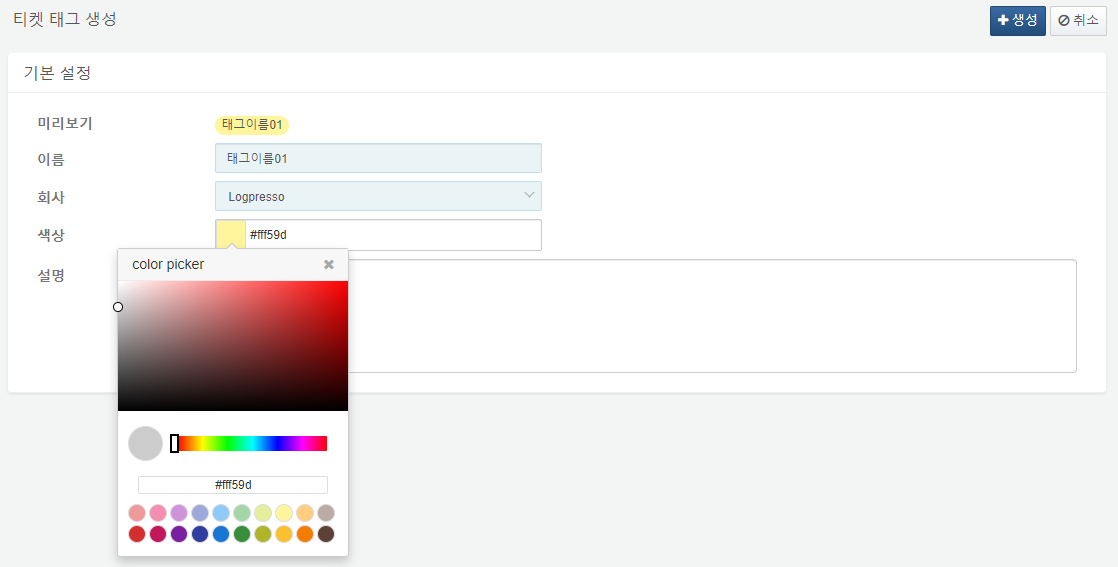
티켓 일괄 작업 중 상태 변경, 정오탐 변경, 사고 여부 변경 시 메모 입력 기능을 추가하였습니다.

메모 입력 모달에서 미입력 시 상태만 변경됩니다.

* 목록에서 티켓 선택 후, 작업 선택: 상태 변경, 정오탐 변경, 사고 여부 변경
* 메모 입력 모달: 미입력 시 상태만 변경
* 티켓 조회: 상태 변경 및 메모 입력 처리

#### SNR#1965 티켓 태그 기능 추가

티켓 분류 및 작업 등에 다양하게 활용할 수 있도록 티켓에 태그 기능을 추가하였습니다.

* 티켓 목록에서 태그 적용: 태그 적용 작업을 통해 티켓에 태그 적용, 적용된 태그는 티켓 제목 우측에 각각 표시됨
* 태그가 적용된 목록 검색: 태그 클릭 시 해당 태그가 적용된 티켓 목록 검색
* 티켓 조회에서 태그 적용: 태그 패널에 적용된 태그 표시, 수정 버튼 클릭 후 적용/해제
* 티켓 태그 관리: 티켓 일괄 작업 및 티켓 조회의 태그 편집을 선택 시 티켓 태그 관리 팝업 표시
* 티켓 태그 생성/편집: 미리보기를 확인하면서 이름과 색상 설정

#### SNR#2011 사용자 정의 필터 객체 및 matchfilter 함수 지원

#### SNR#2080 테이블 데이터 복구 과정에서 데이터 파일 헤더가 손상되는 문제 해결

로그프레소를 시작할 때 테이블 데이터 정합성 확인 단계에서 로그 파일을 복구하면서 생성된 데이터 블록이 낮은 확률로 파일 헤더를 덮어쓰면서 해당 일자 데이터가 조회되지 않는 문제가 발생하지 않도록 수정했습니다.

#### SNR#2105 수집기 필터 기능 추가

#### SNR#2122 앱 리소스 자동 설치

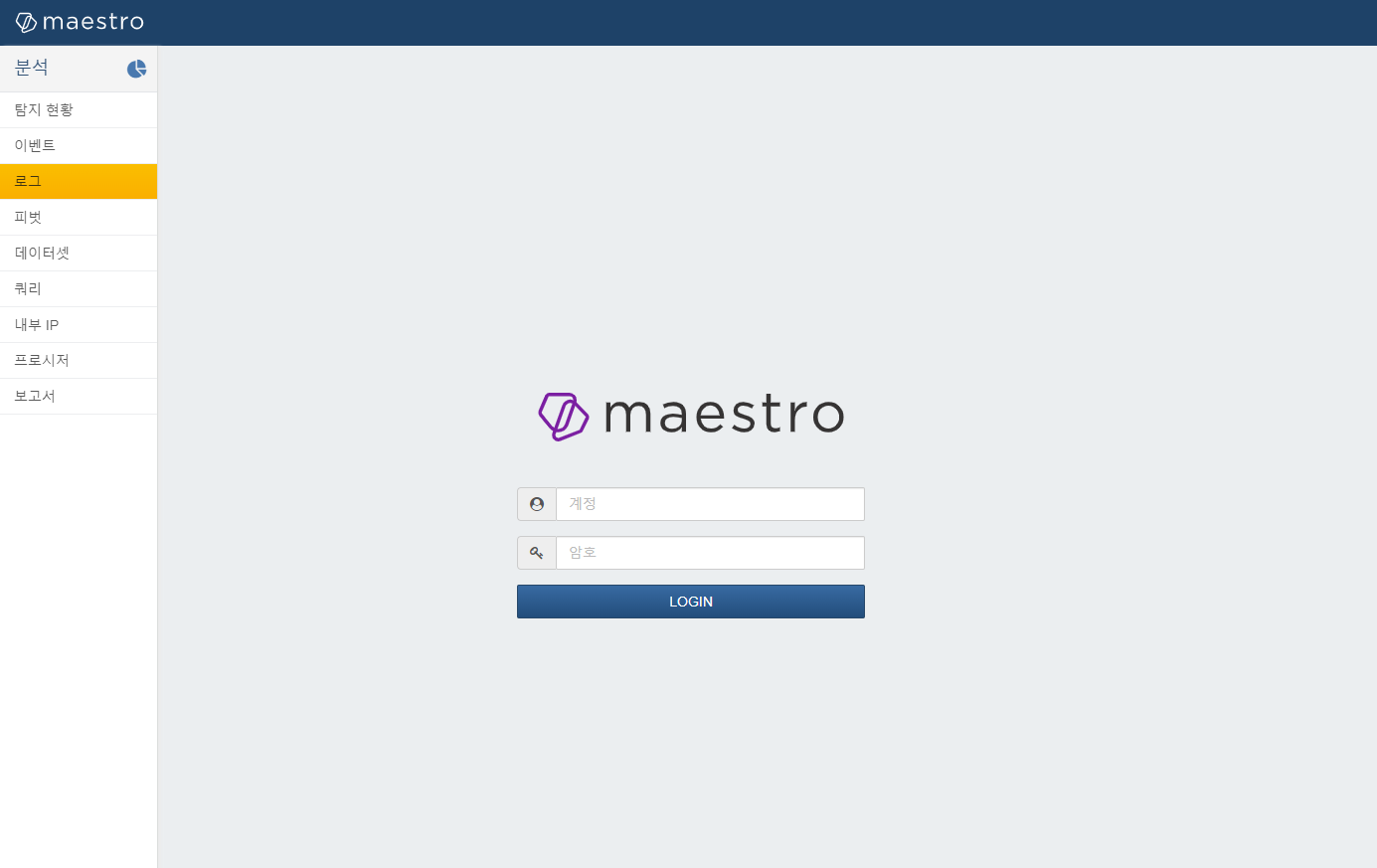
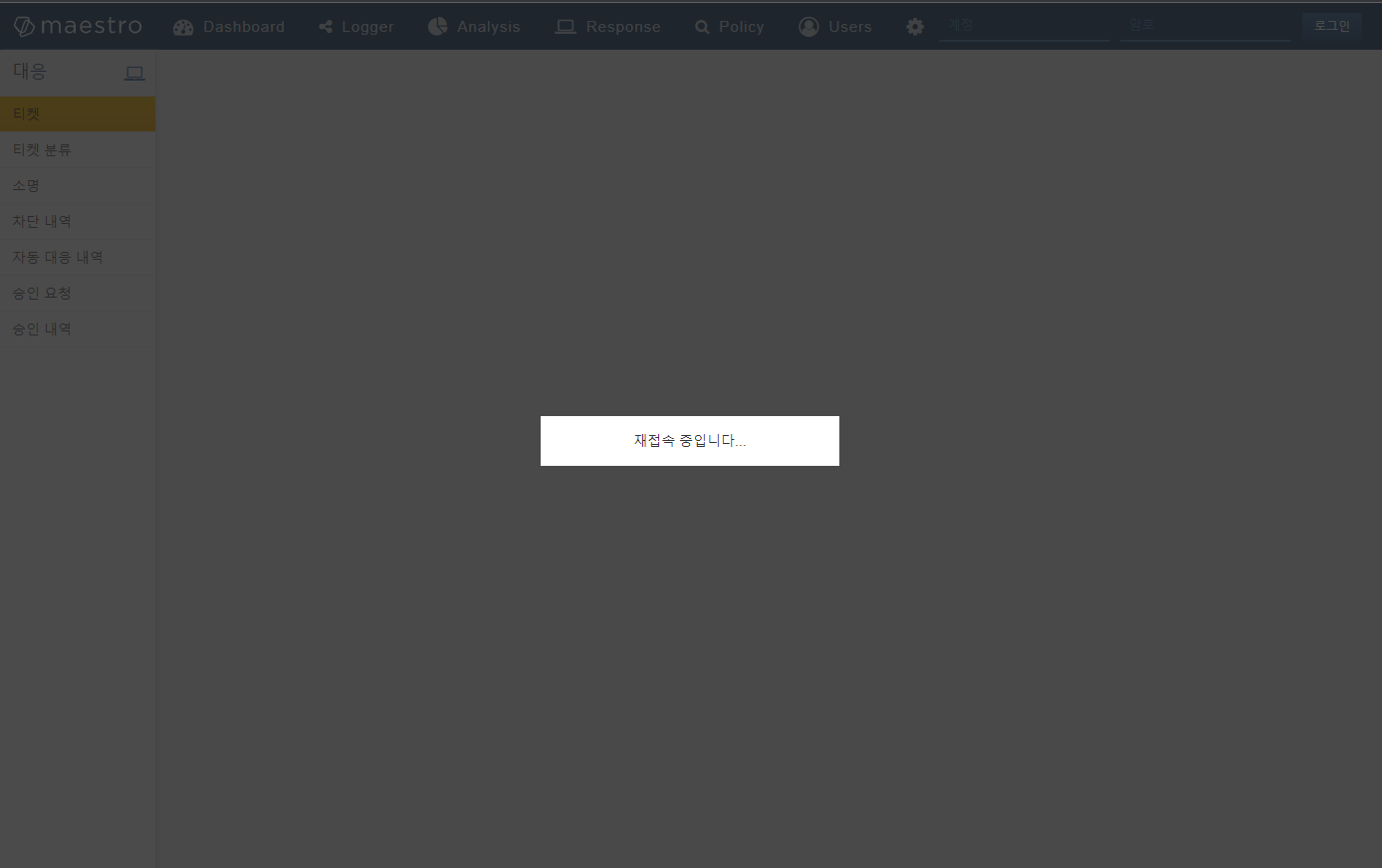
#### SNR#2126 Syslog over TLS 수신 기능 추가

#### SNR#2135 sonar-add-address-batch 명령어 추가

#### SNR#2136 sonar api key 발급 기능 추가

#### SNR#1600 로그인 세션이 유효함에도 로그인 화면이나 "재접속 중입니다" 메시지가 표시되는 문제 해결

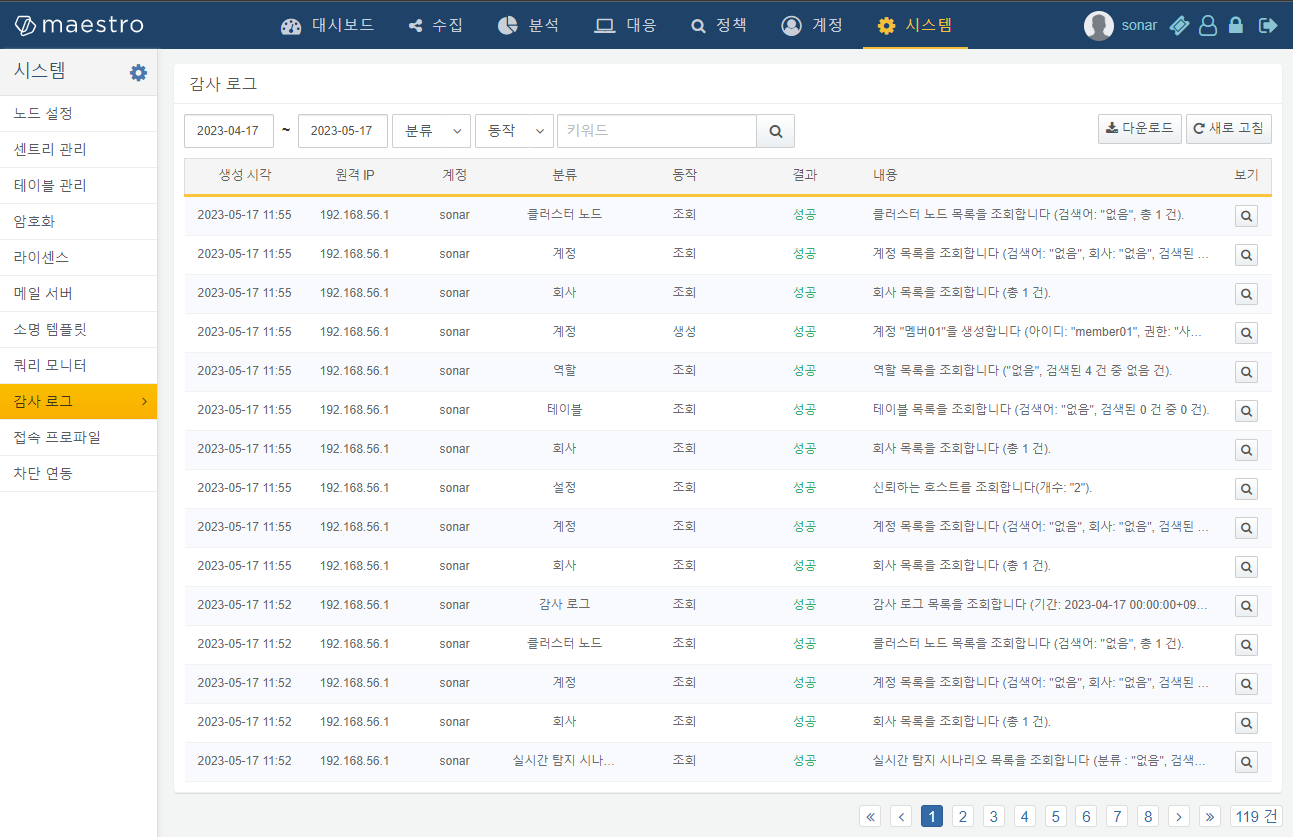
로그인 세션이 유효함에도 네트워크 순단 등의 이유로 아래와 같이 가끔씩 로그인 화면이나 재접속 중입니다... 메시지에서 멈춰있고 브라우저 새로고침을 해야만 정상적으로 화면이 보여지는 문제를 해결하였습니다.

* 로그인 화면이 보여지는 경우
* 재접속 중입니다... 메시지에서 멈춰있는 경우

#### SNR#1625 감사로그 대상 추가 및 감사로그 템플릿 업데이트

설정 변경, 인증 내역 등 추가/수정/삭제에 대해서만 기록하던 감사로그 대상을 화면 조회/다운로드에도 추가 적용하고, 감사로그 템플릿도 함께 업데이트 하였습니다.

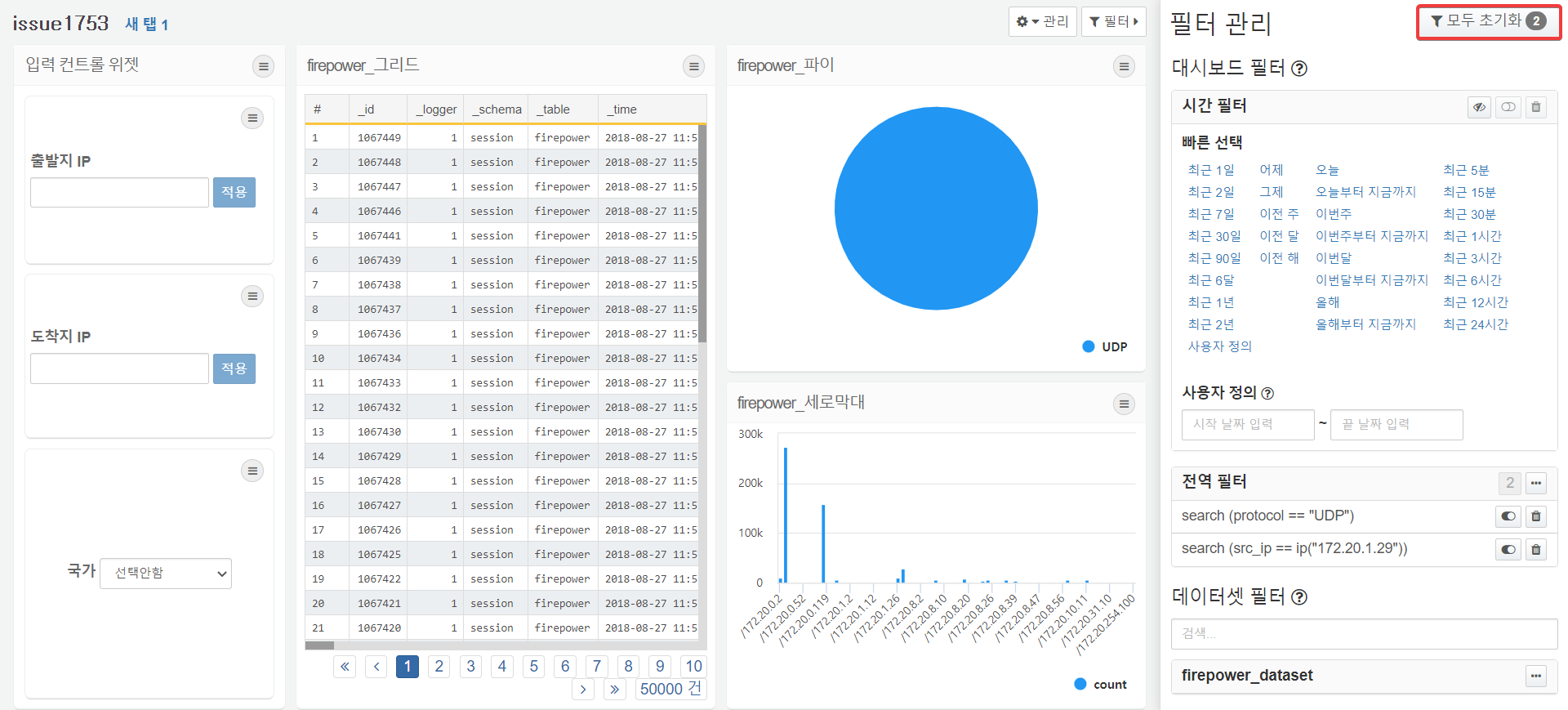
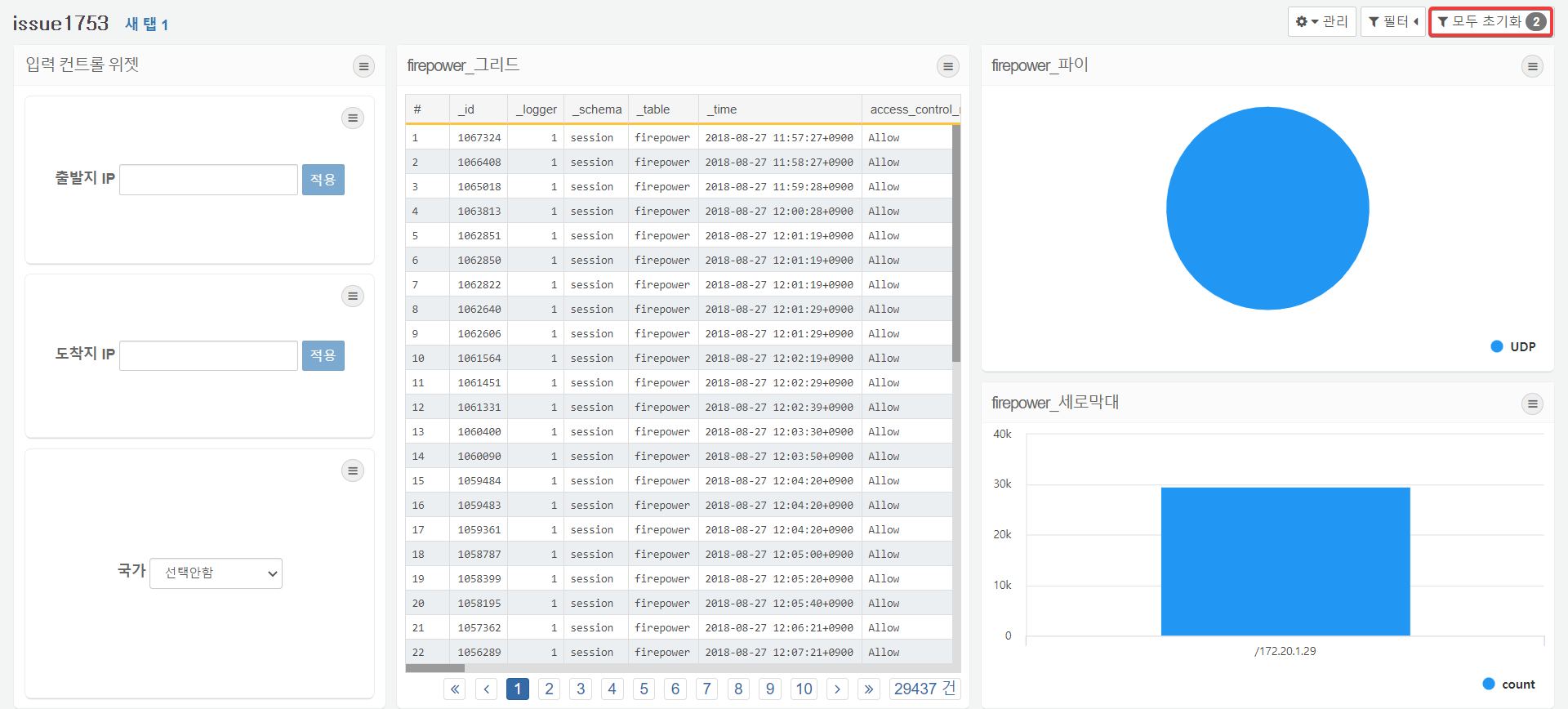
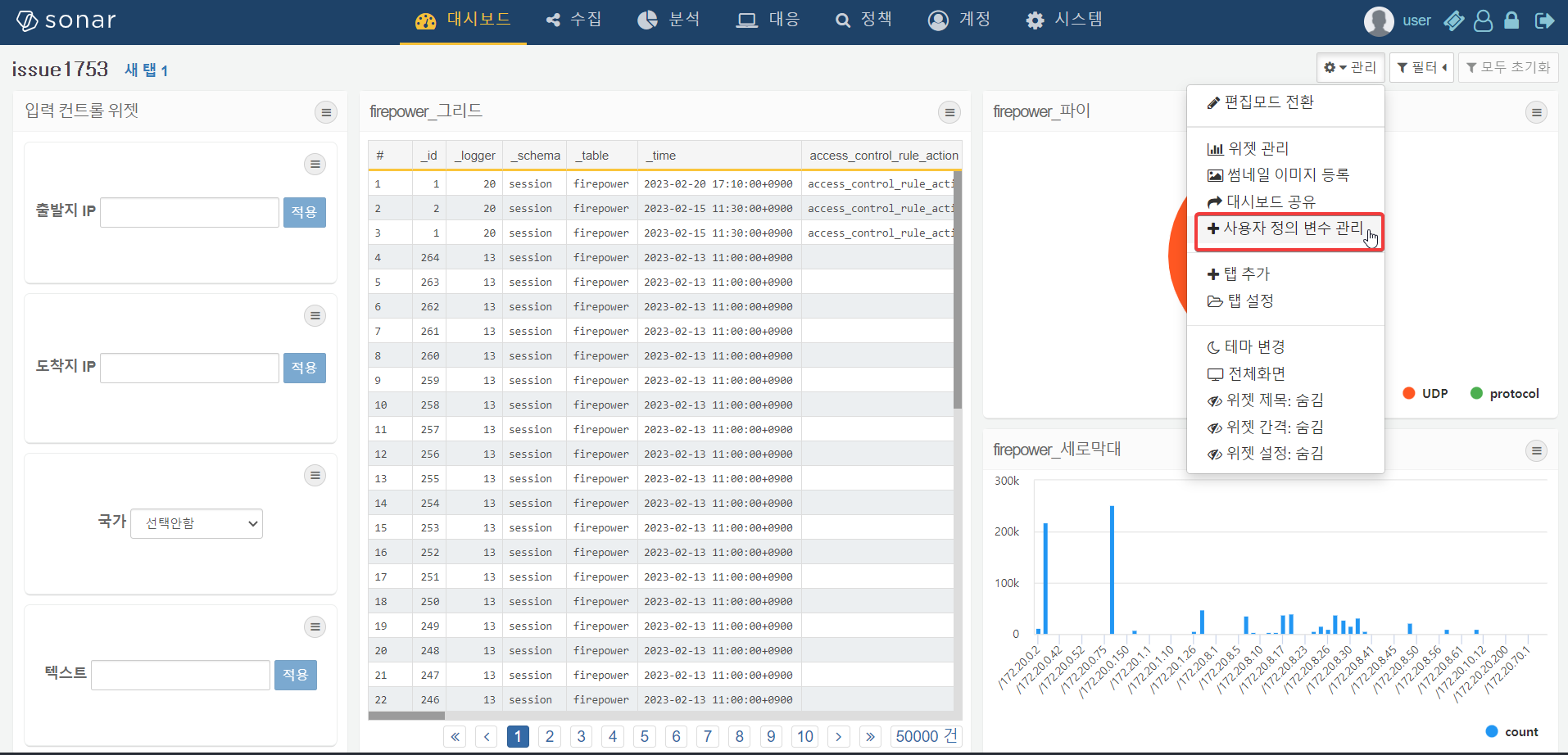
로그인/로그아웃 및 각 화면에서 사용자가 수행하는 추가/수정/삭제/조회/다운로드 등 모든 행위에 대해 감사로그가 기록됩니다.



#### SNR#1753 대시보드 필터 적용/해제 편의성 개선

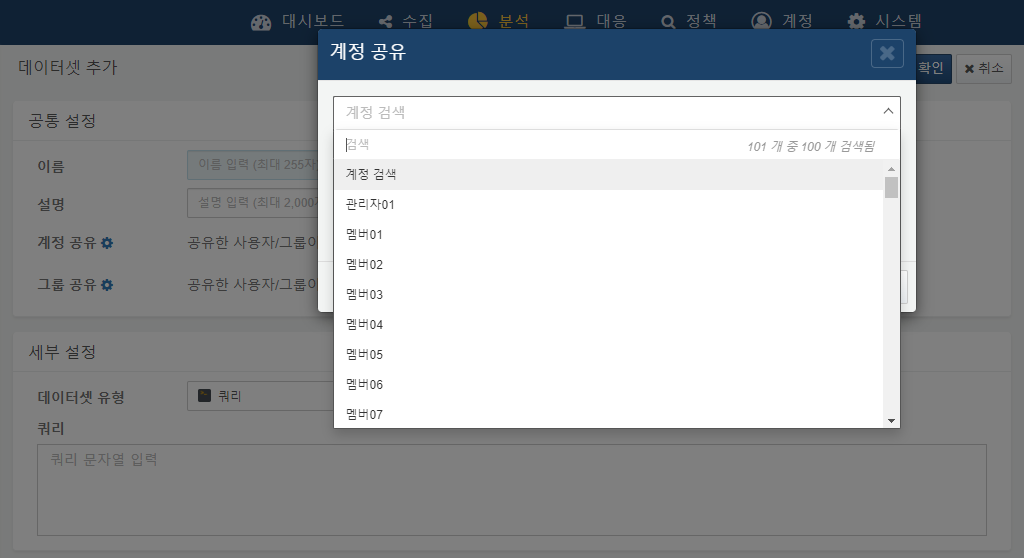
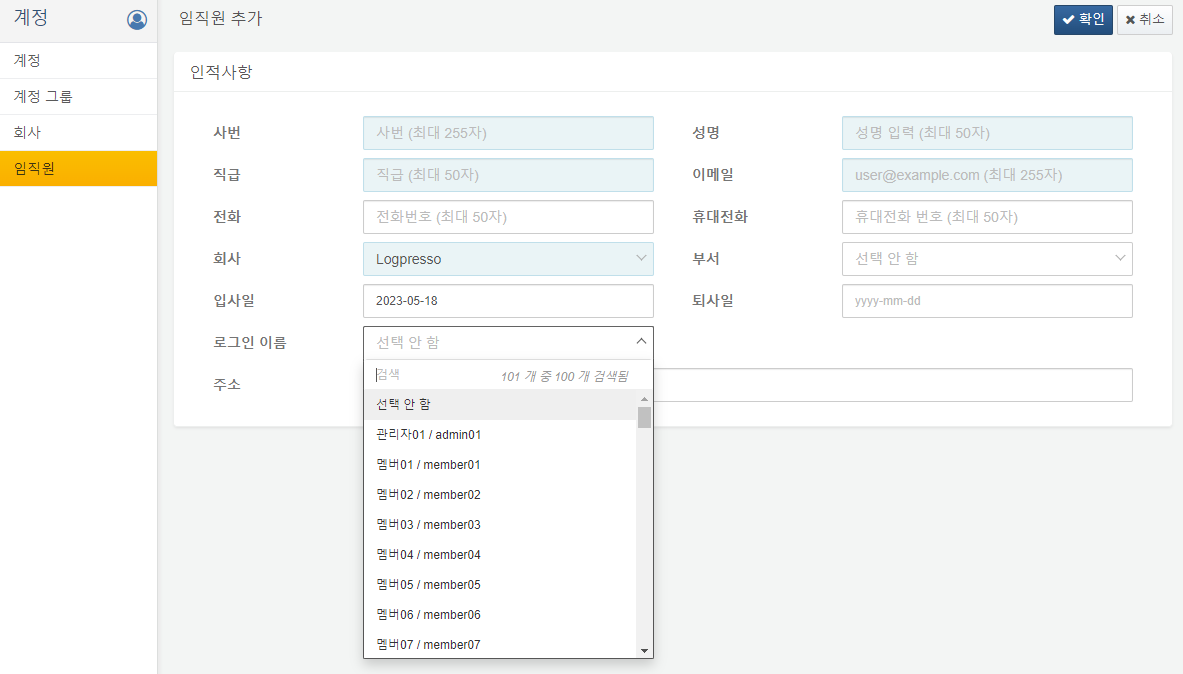
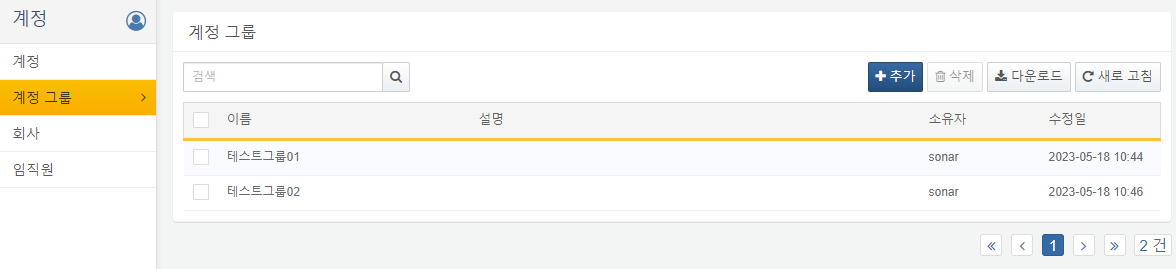
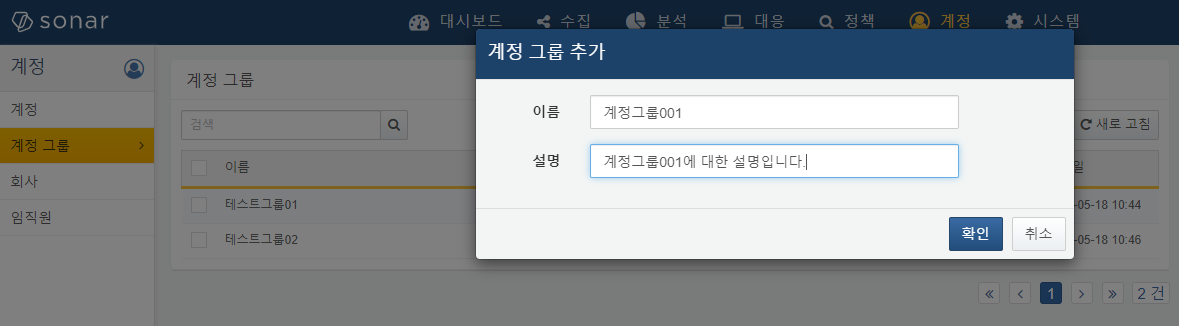
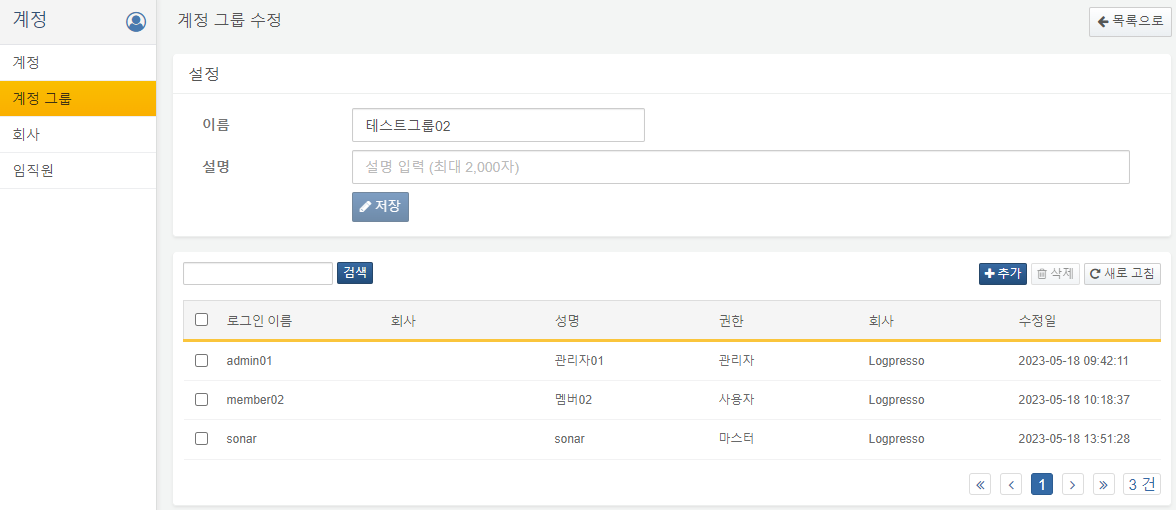
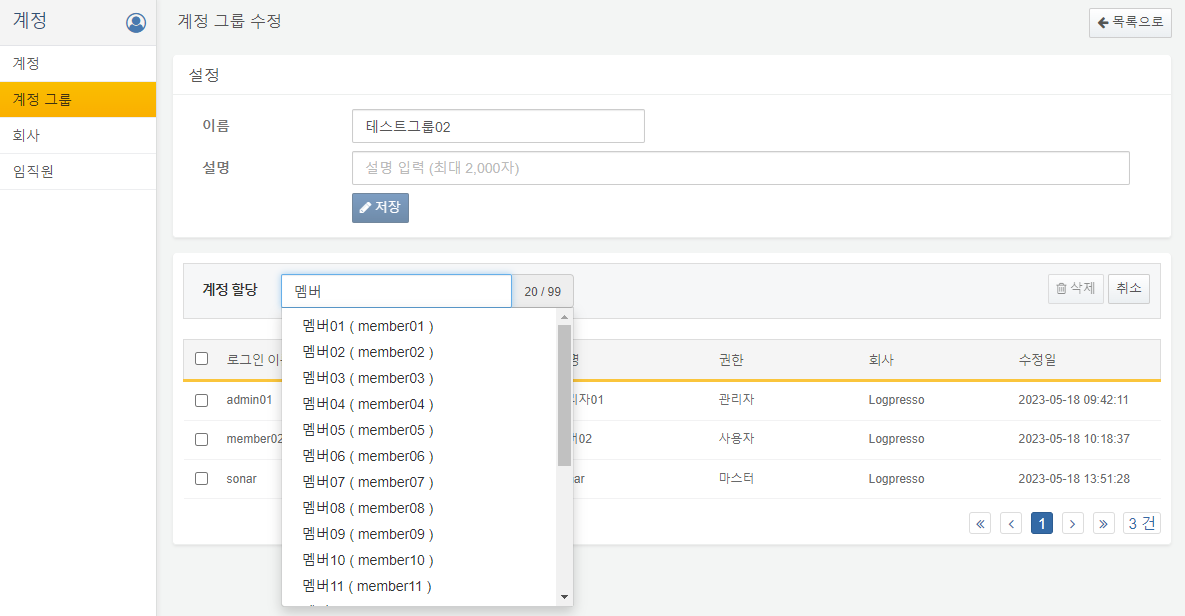
대시보드 필터 관리 패널을 열어서 전체 필터를 해제하던 부분을 모두 초기화 버튼을 상시 표시하고 적용된 필터 개수를 표시하도록 개선하였습니다.

모두 초기화, 필터 패널 토글, 작업 반복, 작업 취소에 대한 단축키를 추가하고, 입력 컨트롤 필터 적용/해제를 위한 사용자 정의 변수 관리 모달을 추가하였습니다.

* 모두 초기화 버튼 상시 표시 및 필터 개수 표시
* 필터 관리 패널이 열린 상태
* 필터 관리 패널이 닫힌 상태
* 모두 초기화, 필터 패널 토글, 작업 반복, 작업 취소 단축키 추가
* 모두 초기화: Ctrl + Q
* 필터 토글: Shift + P
* 작업 반복: Ctrl + Shift + Z
* 작업 취소: Ctrl + Z
* 입력 컨트롤 필터 적용/해제를 위한 사용자 정의 변수 관리 모달 추가

#### SNR#1797 계정 선택 입력 컨트롤 성능 개선

계정 선택을 위해 전체 계정 목록을 조회하던 것을 비동기 방식으로 변경하여 화면 성능을 개선하였습니다.

* 계정 공유: 대시보드, 데이터셋, 프로시저, 접속 프로파일 등
* 임직원 화면: 로그인 이름(계정) 연결
* 계정 그룹 화면: 계정 그룹 관리와 게정 할당 작업을 분리하여 구성
* 계정 그룹 목록
* 계정 그룹 추가
* 계정 그룹에 할당된 계정 목록
* 계정 그룹에 계정 할당

#### SNR#1801 정책 메뉴 화면 일관성 개선

#### SNR#1804 파서 목록 조회 시 권한 점검 제거 및 스크립트 NPE 수정

#### SNR#1824 웹 콘솔 포트를 통한 HTTP POST 로그 수집 지원

이전 버전은 HTTP POST 유형의 수집기가 webconsole HTTP 컨텍스트에 연결되어 있었기 때문에, 로그프레소 엔터프라이즈 웹 포트를 통해서만 HTTP POST 패킷을 수집할 수 있었습니다. 패치 후에는 sonar HTTP 컨텍스트에도 HTTP POST 수집기가 연결되기 때문에, 로그프레소 소나 웹 포트(443/tcp)만 열려있는 환경에서도 웹훅 등 HTTP POST 패킷을 수집할 수 있습니다.

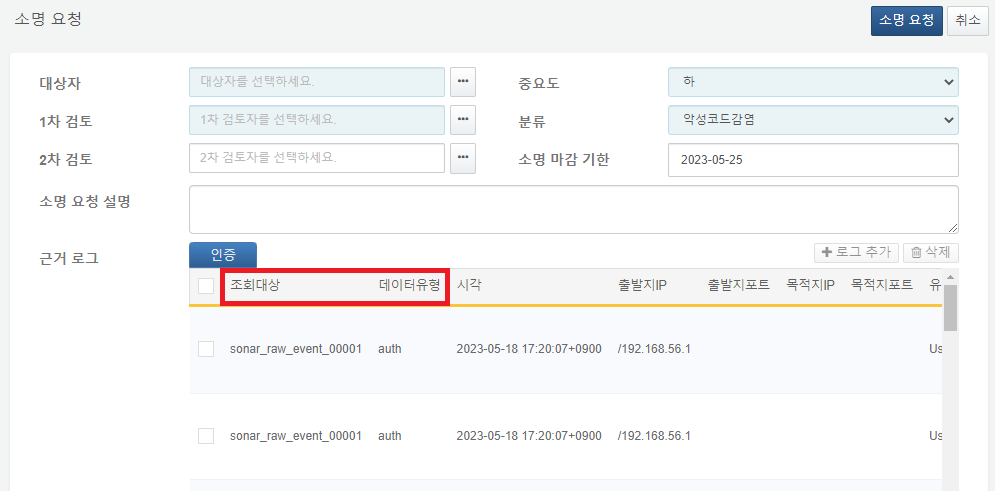
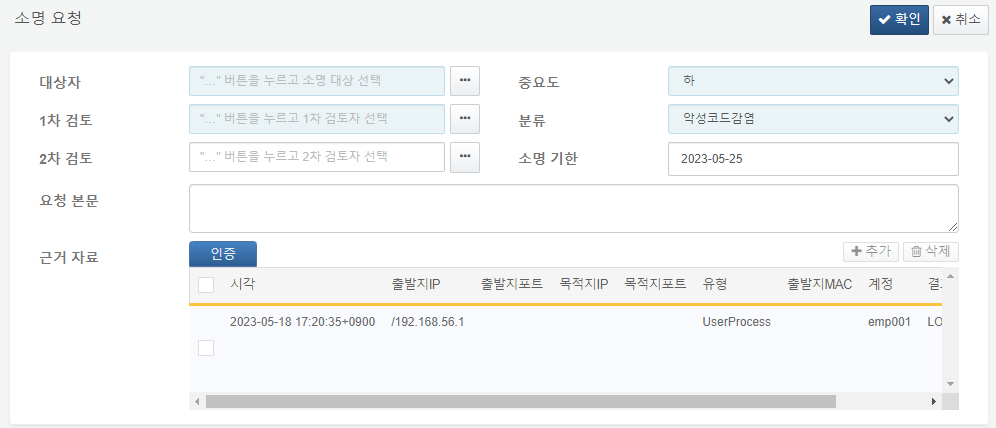
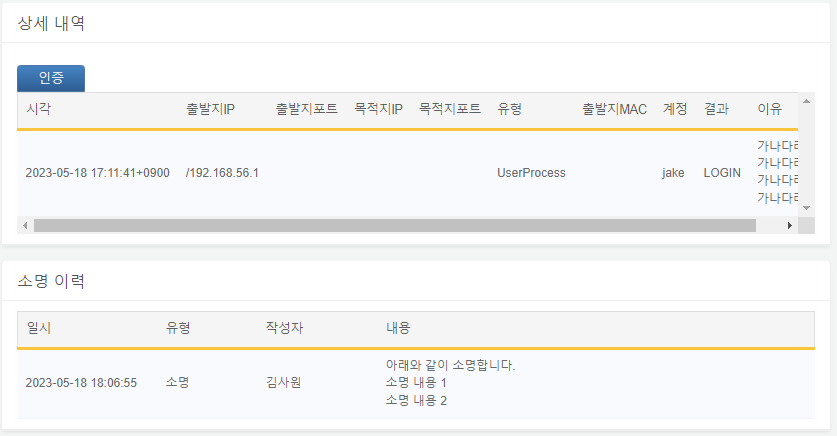
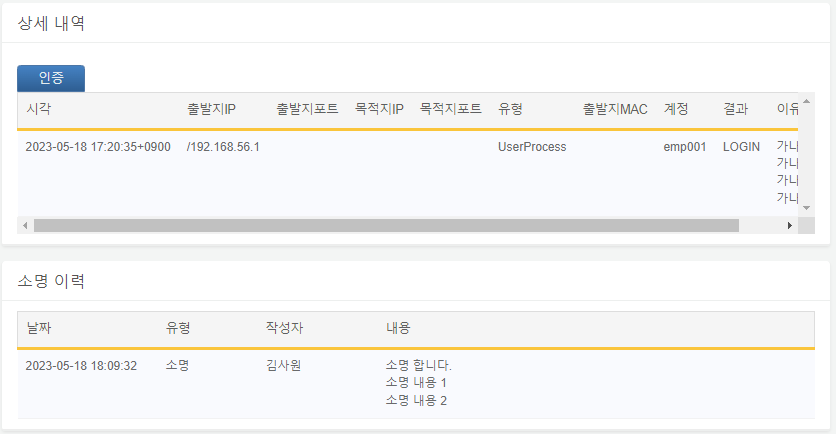
로그프레소 셸에서 아래와 같이 /log/\* 경로에 매핑된 서블릿을 확인할 수 있습니다:

logpresso> httpd.contextsHTTP Contexts---------------HTTP Context [sonar, sessions=0]>>Servlet Context [sonar]\* Context Path=/\* URL Mappings Servlet log /log/\*

#### SNR#1905 소명 화면에서 로그 상단 정렬로 변경 및 근거 자료에 조회대상, 데이터유형 필드 제거

소명 화면에서 상세 내역, 근거 자료, 소명 이력 로그의 표시를 티켓 근거 자료와 일관성을 유지하기 위해 중간 정렬에서 상단 정렬로 변경하였습니다.

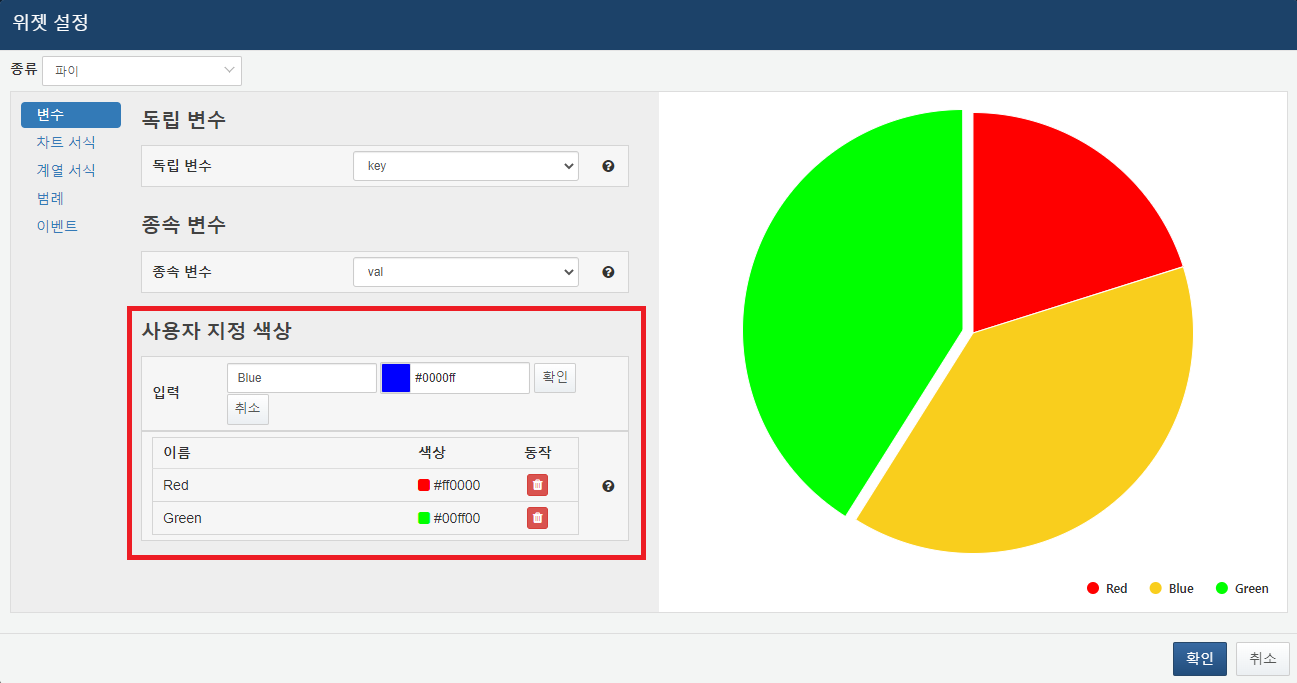
소명 근거 자료에서 소명 업무에 불필요한 조회대상, 데이터유형 필드를 제거하였습니다.

* 소명 근거 자료
* 패치 전: 수직 정렬(중간), 결과 필드(조회대상, 데이터유형 포함)
* 패치 후: 수직 정렬(상단), 결과 필드(조회대상, 데이터유형 제거)
* 소명 상세 내역 및 소명 이력
* 패치 전: 수직 정렬(중간)
* 패치 후: 수직 정렬(상단)

#### SNR#1912 패턴 그룹 상세 페이지의 패턴 목록 컬럼 너비 개선

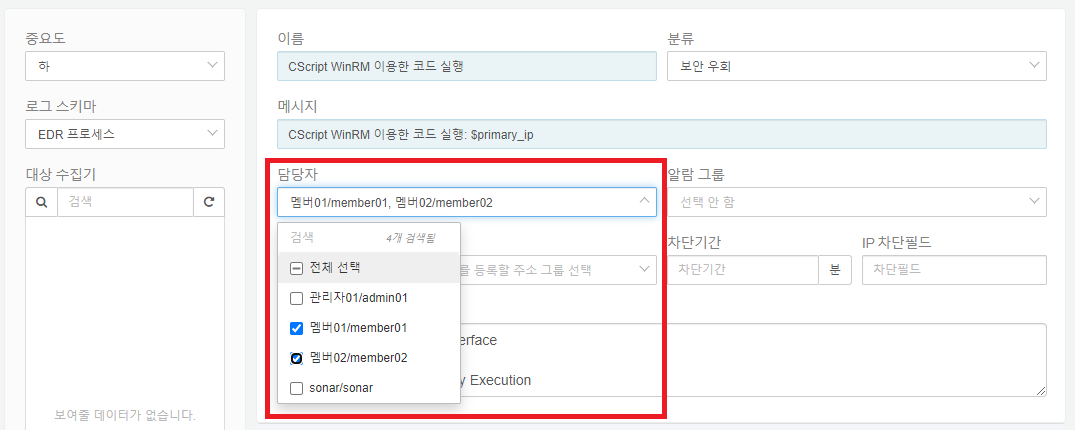
#### SNR#1916 파이 차트 사용자 색상 지정 기능 추가

파이 차트에 사용자 색상 지정 기능이 추가되었습니다. 지정하지 않으면 기본 색상이 사용됩니다.



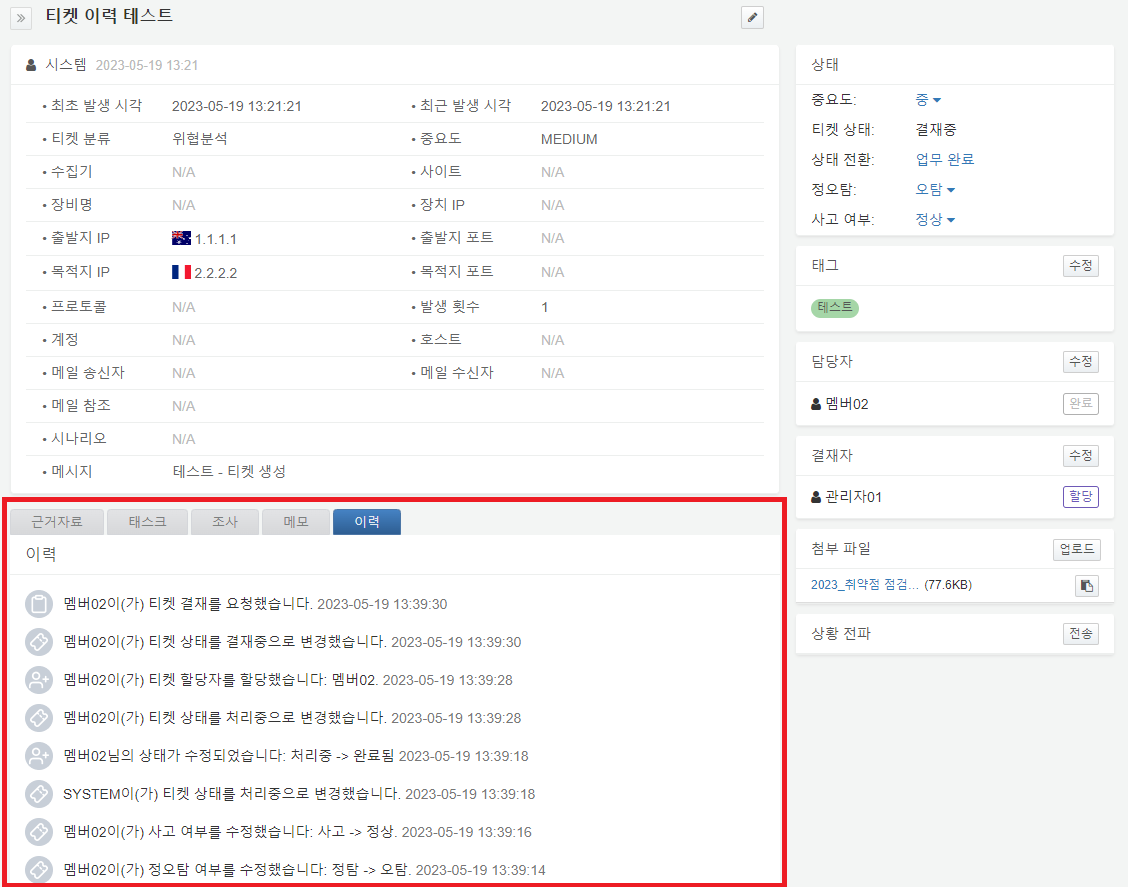
#### SNR#1918 실시간/배치 탐지 시나리오 설정에서 티켓 담당자를 복수 선택할 수 있도록 변경

분석 > 실시간/배치 탐지 시나리오 설정에서 티켓 담당자 할당을 복수 선택할 수 있도록 변경되었습니다.



#### SNR#1938 티켓 작업에 대한 감사 로그 추가

티켓 작업에 대한 감사 로그가 추가되고, 티켓 조회 화면에 이력 탭이 추가되었습니다.



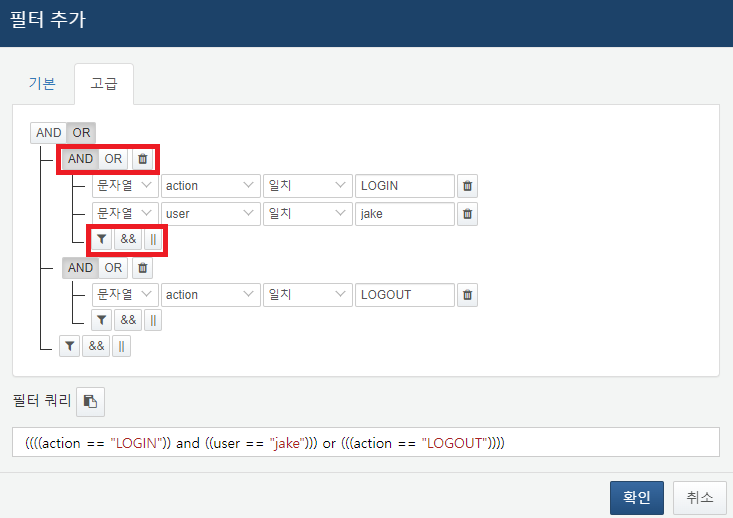
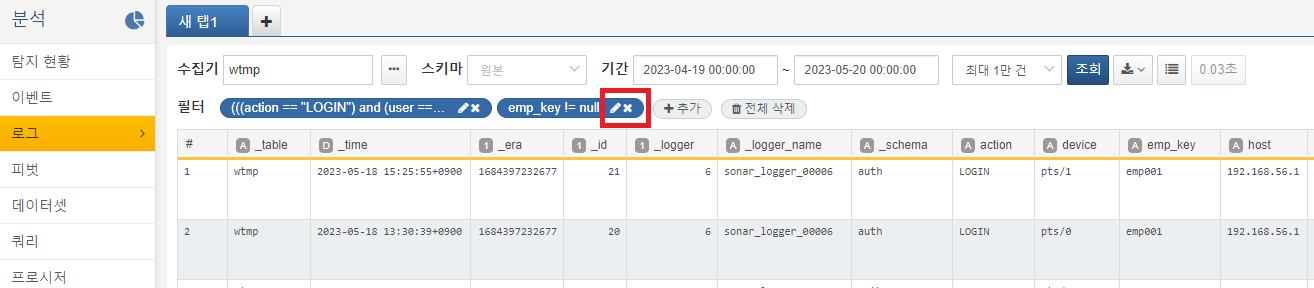
* 감사로그 대상: 티켓 등록/수정, 제목 변경, 상태 변경, 중요도/정오탐/사고 여부 수정, 담당자/결재자 할당, 결재 요청/승인/반려, 첨부 파일 추가/삭제, 메모 추가/수정/삭제, 조사자료 추가

#### SNR#1939 로그 화면 검색 필터 세분화

분석 > 로그 화면 검색 필터가 세분화되었습니다.

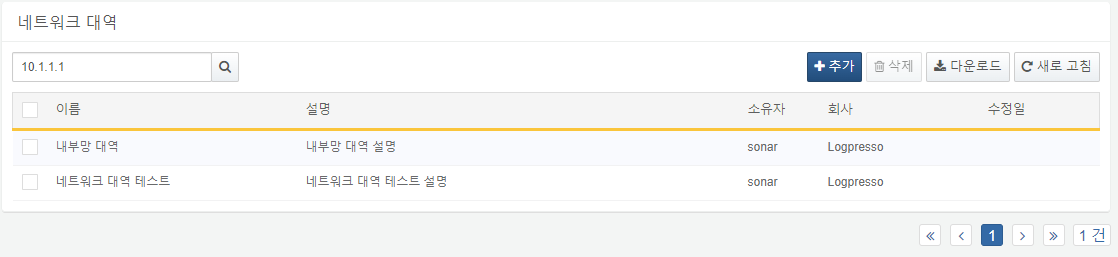
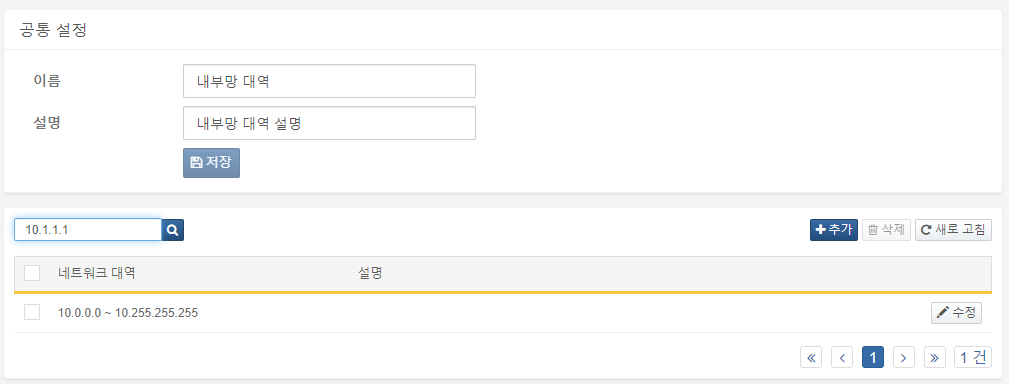
기본 필터에 OR로 여러 값을 설정할 수 있게 추가되었고, 고급 필터 탭에서 세분화된 검색 필터를 설정할 수 있도록 개선되었습니다.

설정된 검색 필터는 필터 쿼리에 표시되고 복사해서 쿼리 화면에서 활용할 수 있습니다.

* 기본 필터: 대상 필드를 선택하도록 변경, 여러 값들을 OR로 설정할 수 있게 추가됨
* 고급 필터: 중첩된 필터를 AND, OR 논리식으로 설정
* 하위 항목 논리식 표현: AND, OR
* 필터 그룹 및 항목 추가: 그룹은 최대 4-depth까지 설정 가능
* 필터 아이콘: 필터 그룹 내 항목 추가
* &&: 하위 AND 그룹 추가
* ||: 하위 OR 그룹 추가
* 로그 화면: 각 필터 조건은 기존처럼 AND로 동작, 기본/고급 필터 설정 항목은 편집 버튼을 클릭하여 수정 가능

#### SNR#1940 네트워크 대역 IP 검색 지원

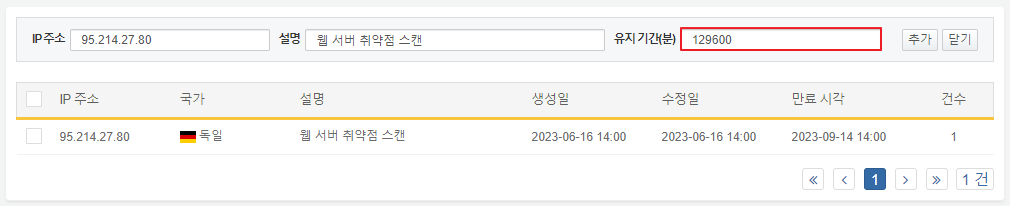
네트워크 대역 그룹 목록 및 네트워크 대역 목록 화면에 IP 주소 검색 기능이 추가되었습니다.

* 네트워크 대역 그룹: IP 주소, 네트워크 대역 그룹 이름, 네트워크 대역 그룹 설명
* IP 주소: 전체 그룹 중 해당 IP를 포함하는 네트워크 대역 그룹
* 공백으로 구분된 검색어들은 AND 조건으로 동작
* 네트워크 대역: IP 주소, 네트워크 대역 설명
* IP 주소: 단일, 범위, CIDR 중 일치하는 네트워크 대역
* 공백으로 구분된 검색어들은 AND 조건으로 동작

#### SNR#1943 표시 개수 조절 컴포넌트 통일 및 내부 IP 화면에 표시 개수 조절 기능 추가

#### SNR#1955 주소 그룹 항목 유지 기간 추가

이전 버전의 'IP 블랙리스트'가 '주소 그룹'으로 명칭이 변경되었습니다. 주소 그룹은 차단 연동 설정으로 방화벽과 같은 보안 장비에 연동시키는 경우가 많습니다. 일반적으로 차단 설정할 수 있는 IP 주소의 갯수에는 한계가 있기 때문에, 주소 그룹의 수를 적정 수준으로 유지할 필요가 있습니다. 이 때문에 주소 그룹 항목을 추가할 때 유지 기간을 분 단위로 지정하는 기능이 추가되었습니다.



예를 들어, IP 주소를 3개월동안 유지하려면 129600분을 입력합니다. IP 주소에 설정된 만료 시각을 지나면 해당 IP 주소는 자동으로 삭제됩니다.

#### SNR#1963 티켓 화면 편의성 및 성능 개선

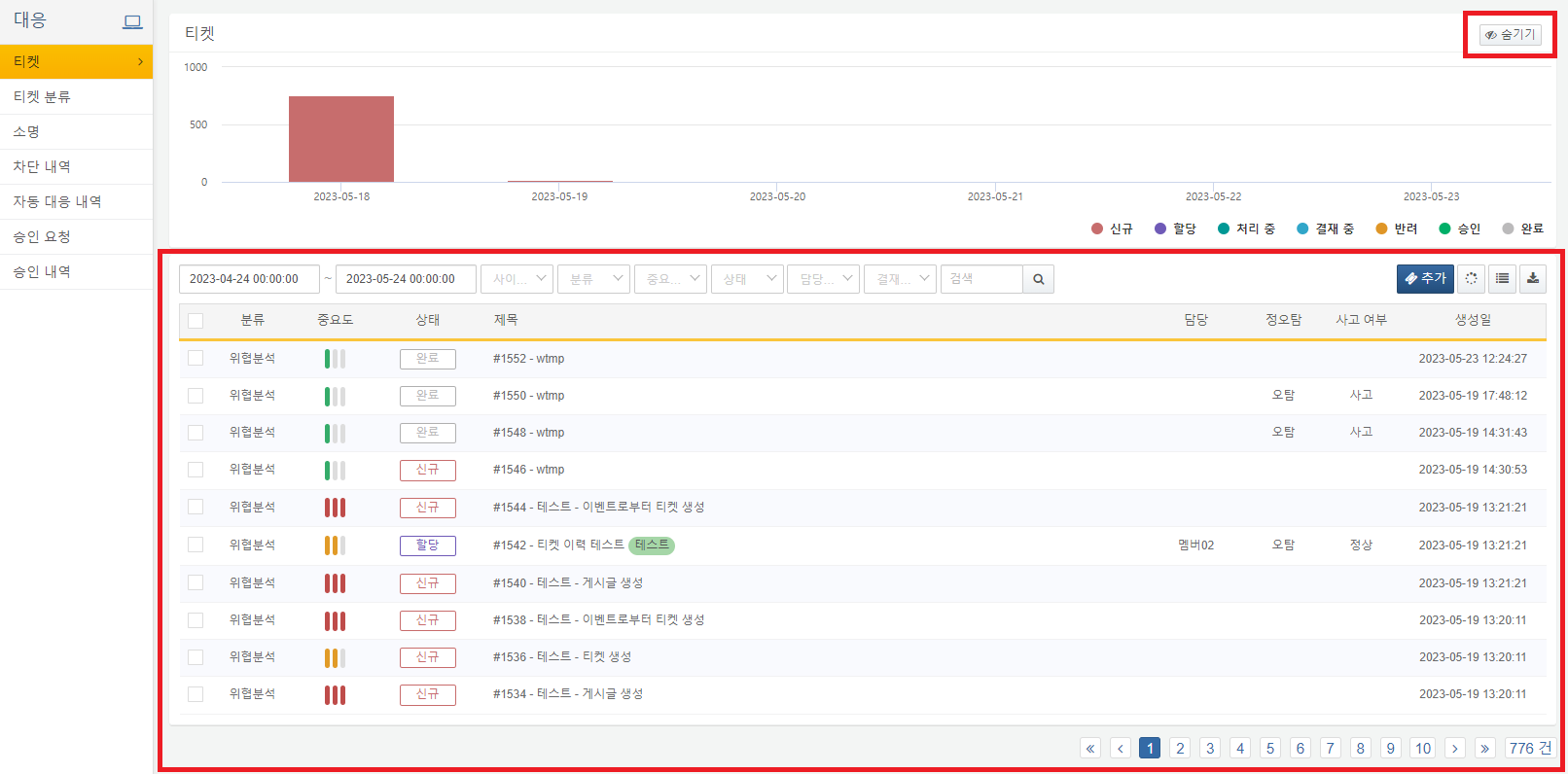
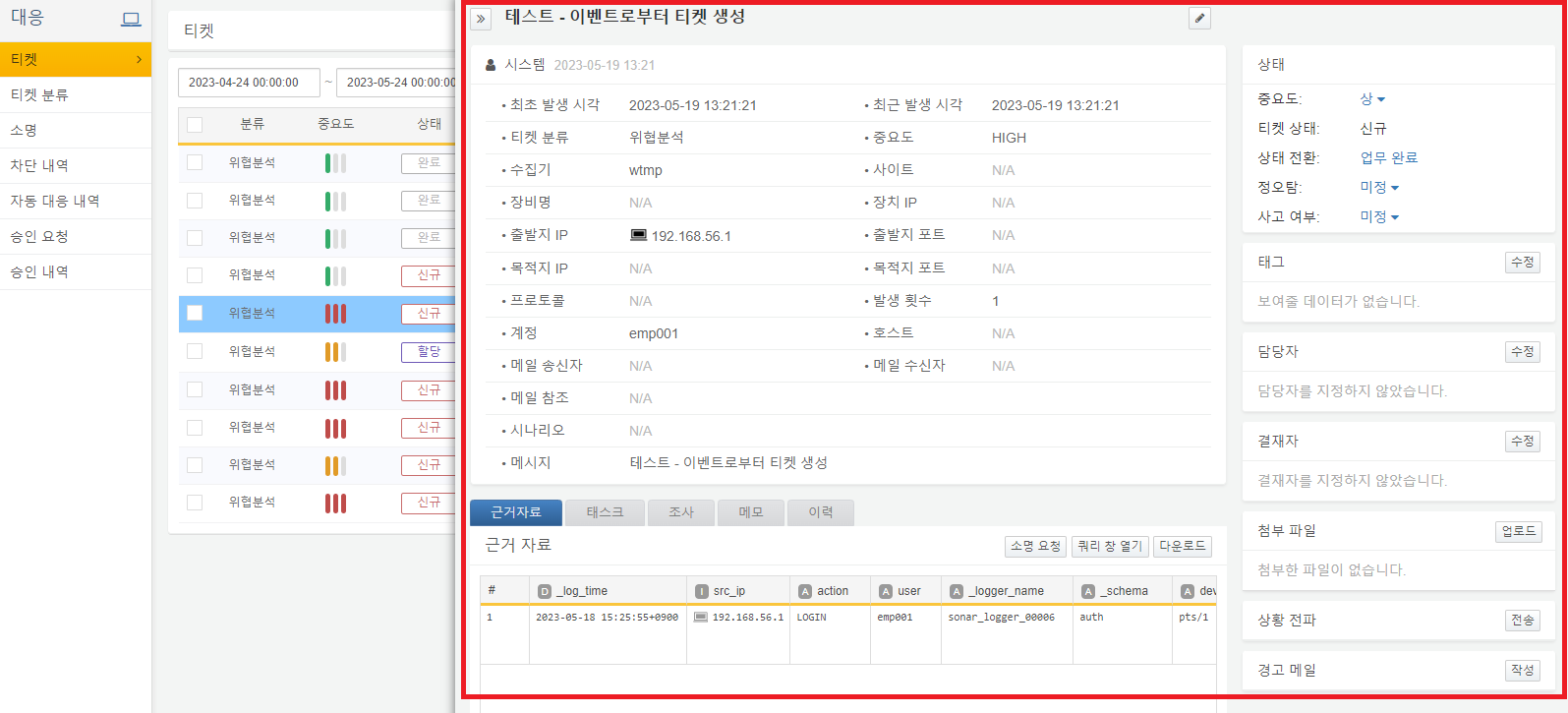
티켓 화면 편의성 및 성능을 개선하였습니다.

티켓 목록 표시: 전체 화면 넓이를 사용하도록 변경

티켓 추이 그래프: 숨기기 기능 추가

티켓 조회 화면: 화면 전환에서 오른쪽 사이드 패널로 표시되도록 변경

화면 성능 개선: 메모리 누수 해소 및 화면 렌더링 성능 개선

* 티켓 목록
* 티켓 목록을 화면 넓이에 따른 가변폭으로 표시
* 티켓 추이 그래프 숨기기/보이기 토글 기능 추가
* 티켓 조회
* 목록에서 선택한 티켓을 오른쪽 사이드 패널에 표시
* >> 버튼 클릭 또는 Esc 키를 입력하면 닫힘

#### SNR#1969 이벤트로부터 티켓 생성 명령어에서 입력 이벤트의 GUID, 시각을 저장하도록 변경

플레이북 이벤트로부터 티켓 생성(maestro-create-ticket-from-event) 명령어에서 입력 매개변수 이벤트 GUID에 해당하는 이벤트의 GUID 및 시각을 저장하도록 변경되었습니다.

* sonar\_event 추가 필드: parent\_guid, parent\_time
* sonar\_raw\_event 추가 필드: \_parent\_guid, \_parent\_time

이벤트 화면 및 탐지현황 화면에서는 해당 이벤트가 조회되지 않도록 쿼리를 수정 반영하였습니다.

* 수정 반영한 쿼리: search isnull(parent\_guid)

이벤트로부터 티켓 생성(maestro-create-ticket-from-event) 및 티켓 생성(maestro-create-ticket) 명령어에서 목적지 IP(dst\_ip)와 호스트(host\_ip)가 출발지 IP(src\_ip) 값으로 잘못 설정되던 버그도 함꼐 수정하였습니다.

#### SNR#2041 동시에 실행되는 배치 시나리오의 개수를 조절하는 시스템 스위치 추가

많은 수의 배치 시나리오가 동시에 실행되면 GC문제가 발생하게 되는데, 시스템 스위치로 동시에 실행되는 배치 시나리오의 개수를 조절하여 이를 개선하였습니다. 동시에 실행되는 배치 시나리오의 개수는 기본값으로 6개이며, 부팅 스크립트에 logpresso.sonar.batch\_rule\_thread\_pool\_size을 추가하여 개수 변경이 가능합니다.

* 시스템 스위치 문법

-Dlogpresso.sonar.batch\_rule\_thread\_pool\_size=6

#### SNR#2066 remote 쿼리 커맨드 벡터화

remote 쿼리 커맨드를 사용하는 로그, 피벗 등의 메뉴에서 대량의 데이터를 조회할 때 극심한 GC가 발생하는 현상이 해결되었습니다.

#### SNR#2074 대형 레코드 수집/쿼리 시 GC 문제 완화

테이블별로 데이터를 플러시 하는 건수를 지정하는 기능이 추가되었습니다.(현재 데이터 플러시 건수는 기본 2000건 입니다.)

TABLE\_NAME 테이블에 대해 기본 건수를 INTEGER 개로 설정하는 명령입니다.

logstorage.setEngine v3p flush\_count.TABLE\_NAME INTEGER

예를 들어 maili 테이블의 플러시 건수를 100건으로 설정하는 명령은 다음과 같습니다.

logstorage.setEngine v3p flush\_count.maili 100

현재 수집중인 테이블의 경우 다음 명령을 사용해 설정을 반영할 수 있습니다.

logstorage.sweep TABLE\_NAME1 TABLE\_NAME2 ...

대형 레코드 위주로 저장되는 테이블에선 기본 2000건을 기준으로 플러시 하면 메모리 사용량이 크게 증가하여 GC를 유발합니다.이런 테이블들에 대해 더 적은 건수로 플러시 건수를 지정한다면, GC가 완화됩니다.

참고로 현재 설정은 다음 명령어로 확인할 수 있습니다.

logsorage.engineConfigs v3p

#### SNR#2075 파일 수집 시, 사용자 정의 개행문자 지원

파일 수집 시, 개행 문자를 사용자가 직접 정의할 수 있도록 개선하였습니다.

* 파일 수집 시, 사용자 정의 개행 문자 지원

#### SNR#2077 리눅스 일반 사용자 권한으로 데몬 구동시 NTP 동작 실패하는 문제 해결

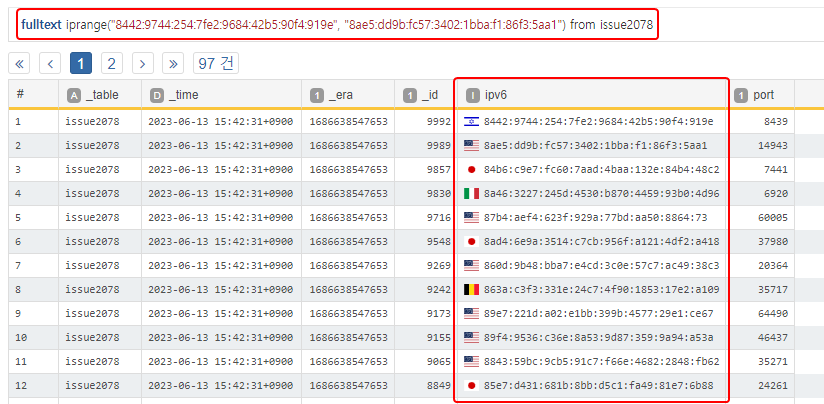
리눅스 일반 사용자 권한으로 데몬 구동시 NTP 동작 실패하는 문제를 해결하였습니다.

#### SNR#2078 fulltext 커맨드 IPv6 타입 검색 지원

fulltext 커맨드가 IPv6 타입 검색을 지원합니다. 그에 따라 IP 관련 함수가 추가 및 변경되었습니다.

**fulltext 커맨드 IPv6 타입 검색 지원**

fulltext 커맨드가 IPv6 타입 검색을 지원합니다.

* fulltext IPv6 검색

**IP 관련 함수 추가, 변경 사항**

* (변경) ip()
* 단일 ipv6 문자열 주소도 받을 수 있도록 변경되었습니다.
* 예시: src\_ip == ip('fe80::85d:e82c:9446:7995')
* (변경) iprange()
* ipv6 문자열 주소 범위도 받을 수 있도록 변경되었습니다.
* 예시: src\_ip == iprange('fe80::85d:e82c:9446:7995', 'fe80::85d:e82c:9446:79a0')
* (추가) ipv6()
* 단일 주소 처리 : src\_ip == ipv6('fe80::85d:e82c:9446:7995')
* 패턴 처리: 패턴을 받아 해당되는 범위를 검색합니다.
* 예시
* src\_ip == ipv6('fe80::85d::9446:/64')
* src\_ip == ipv6('fe80::85d:e82c:9446:7995', 127)
* (추가) isv4linklocal()
* 인자로 받은 필드가 v4 type link local address(예: 169.254.0.0~169.254.255.255) 토큰인지 확인하는 조건 함수입니다.
* 예
* isv4linklocal(src\_ip)
* not isv4linklocal(src\_ip)
* (추가) isv6linklocal()
* 인자로 받은 필드가 v6 type link local address(예: fe80::/10) 토큰인지 확인하는 조건 함수입니다.
* 예
* isv6linklocal(src\_ip)
* not isv6linklocal(src\_ip)

#### SNR#2079 Syslog 정규식 필터 매칭 병렬화

시스로그 수집기에 정규식 필터를 설정했을 때, 시스로그 유입양이 많은 경우 성능 저하가 생겨 유실이 발생하는 경우가 있었습니다.정규식 필터 매칭을 병렬화 해 성능이 가속되어 이 문제를 개선했습니다.

#### SNR#2101 GeoIP 데이터베이스 업데이트 반영

#### SNR#2110 보안이 강화된 최신 리눅스 배포판(RHEL 9 등)에서 SSH CLI 가 접속되지 않는 문제 해결

보안이 강화된 최신 리눅스 배포판(ex: RHEL 9 등)에서 SSH CLI 가 접속되지 않는 문제를 해결하였습니다.

#### SNR#2107 클라이언트와 서버의 시간 차이 오류 메시지 개선

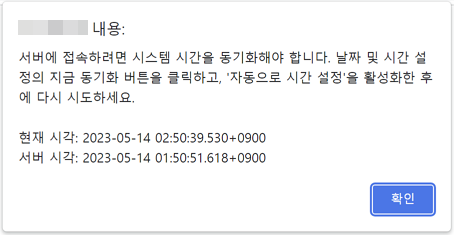
로그프레소 서버는 암호화된 웹소켓 메시지의 리플레이 공격을 방지하기 위하여 서버의 현재 시각과 5분 이상의 차이를 허용하지 않습니다. 하지만 이전에는 오류 메시지에 클라이언트와 서버의 현재 시각만 표시되어 무엇이 문제인지 사용자가 이해하기 어려웠습니다.

최신 버전은 사용자가 어떻게 해야 로그프레소 웹 콘솔에 접속할 수 있는지 명확한 지침을 제공합니다.

**패치 전 메시지**



**패치 후 메시지**



#### SNR#2132 geomac 룩업 데이터 업데이트

geomac 룩업은 MAC 주소를 네트워크 카드 제조사의 이름과 국가로 변환하는 기능을 제공합니다. 로그프레소는 [IEEE](https://standards-oui.ieee.org/oui/oui.txt)에서 배포하는 MAC 주소의 OUI(Organizationally Unique Identifiers) 목록을 정규화하여 사용합니다. 최신 룩업 데이터는 이전 버전보다 1.7배의 목록을 포함합니다.

#### SNR#2133 소나 명령어 도움말 및 에러 처리 정리

#### SNR#2134 event 쿼리 명령어에 duration, order 옵션 추가

event 쿼리 명령어에 duration 및 order 옵션을 추가했습니다.

최근 24시간 이벤트 목록 조회

event duration=1d

최근 10분 이벤트를 오래된 순서대로 조회

event duration=10m order=asc

#### SNR#2139 이중화 로직 개선

#### SNR#1324 검색 창에서 `\_`, `%`, `` 문자열이 정상적으로 검색되지 않는 문제 해결

검색 창에서 \_, %, \ 문자열을 포함해서 검색하면 의도한 검색 결과가 나오지 않는 문제가 해결되었습니다. 기존 버전에서는 \_와 %의 경우 와일드카드, \를 이스케이프 문자열로 인식하였던 문제가 있었으며 패치 후에는 각 문자열을 있는 그대로 검색합니다.

#### SNR#1433 목록 화면에서 아무 항목을 선택하지 않아도 삭제 버튼이 활성화되는 문제 해결

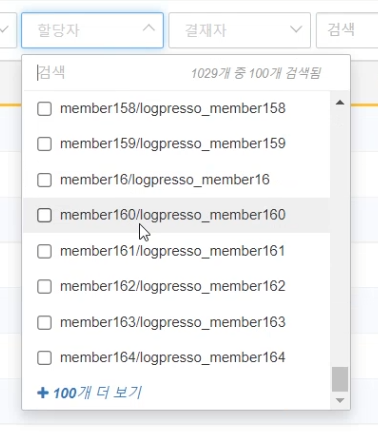
위젯 관리, 머신러닝 모델, 행위 프로파일, 학습 데이터셋, 계정 목록 화면에서 아무 항목을 선택하지 않아도 삭제 버튼이 활성화되어있던 문제가 해결되었습니다.

#### SNR#1465 티켓 분류 삭제 시 삭제되지 않는 티켓 분류도 삭제되었다고 메시지가 표시되는 문제 해결

탐지 정책에서 사용 중인 티켓 분류는 삭제가 불가능하지만, 티켓 분류 삭제 시 분류 삭제에 성공했습니다. 라고 메시지가 표시되는 문제가 해결되었습니다. 패치 후 탐지 정책에서 사용 중인 티켓 분류를 삭제하려고 하면 삭제할 수 없다는 메시지가 표시되며 삭제를 할 수 없습니다.

#### SNR#1616 소나 계정이 매우 많을 때 티켓 목록 조회가 느려지는 문제 해결

소나 계정이 1000개 이상 있는 경우 티켓 목록 화면이나 임직원 추가 화면에서 계정 선택 드롭박스를 선택할 때 전체 계정 목록을 표시하려고 하면서 브라우저 화면이 느려지는 문제가 해결되었습니다. 패치 후에는 계정 선택 드롭박스에서 모든 계정이 표시되지 않고 한 번에 100개씩 표시하며, 계정 검색 기능이 추가되었습니다.



#### SNR#1719 탐지현황 메뉴에서 분류 항목을 일부 해제했다가 다시 전체 선택하는 경우 그래프 색상이 중복되어 표시되던 문제 해결

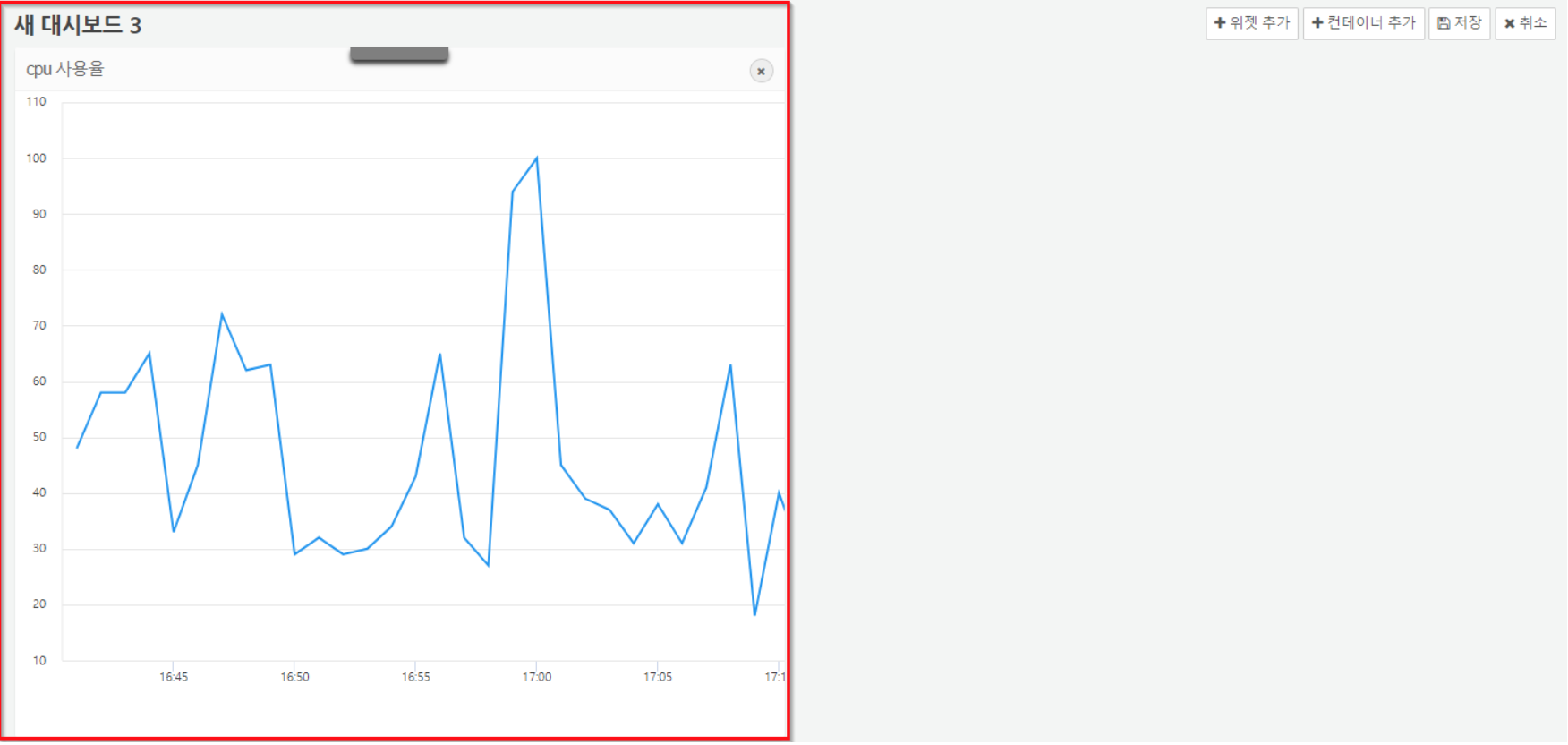
탐지현황 메뉴에서 분류 항목을 일부 해제했다가 다시 전체 선택하는 경우 탐지 현황 그래프의 색상이 중복되어 표시되던 문제가 해결되었습니다.

#### SNR#1763 위젯 생성시 필수 항목을 설정하지 않아도 위젯을 저장할 수 있는 문제 해결

위젯 생성시 독립변수, 종속변수 등 필수 항목을 설정하지 않아도 위젯을 저장할 수 있는 문제를 해결했습니다.

#### SNR#1764 대시보드의 첫 위젯을 도킹하면 대시보드 영역의 반이 사용할 수 없는 상태로 변하는 문제 해결

대시보드에 첫 위젯을 추가한 후 드래그하여 상하좌우 중 한 쪽에 도킹하면 대시보드 화면 영역의 반만 사용할 수 있고 나머지 반은 사용할 수 없었던 문제가 해결되었습니다.

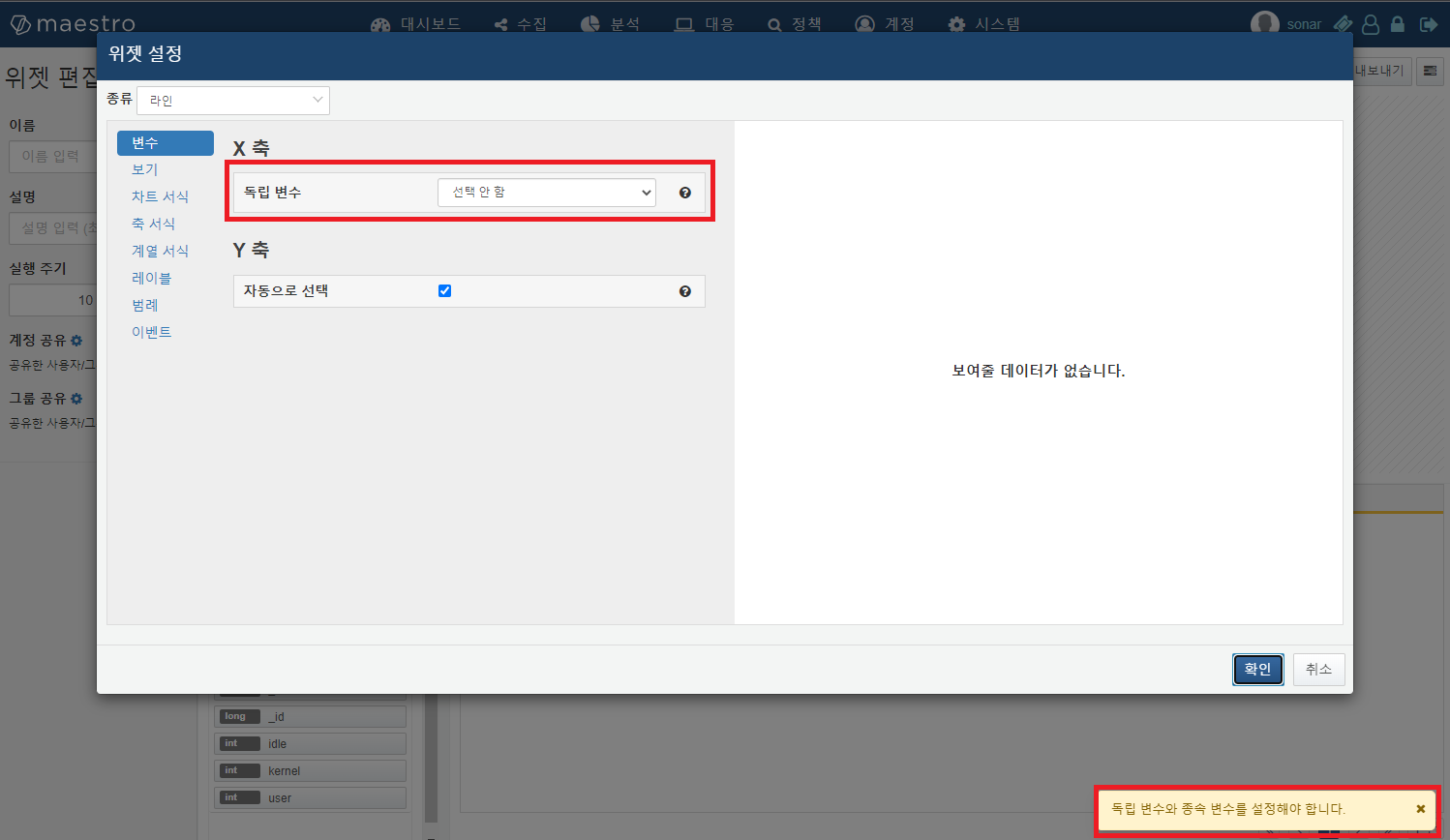
* 패치 전: 위젯이 하나밖에 없으나 대시보드 화면의 왼쪽 반만 사용 가능

#### SNR#1765 대시보드 제목 수정 취소 시 변경에 실패했다는 메세지가 표시되는 문제 해결

대시보드 제목을 수정하다가 취소 버튼을 눌렀는데 변경에 실패했다는 메시지가 표시되는 문제가 해결되었습니다. 패치 후 제목 수정 취소 시 정상적으로 아무런 메시지도 표시되지 않습니다.

#### SNR#1769 위젯 설정에서 유효성 검사 메시지가 제대로 표시되지 않는 문제 해결

위젯 설정에서 독립 변수가 설정되지 않았을 때, 유효성 검사 메시지가 제대로 표시되지 않는 문제를 해결하였습니다.

* 독립 변수 미설정으로 인해 문제가 발생한 동작
* 위젯 설정 화면 진입 후, 바로 적용 버튼을 클릭했을 때
* 경고상자 위젯에서 위젯 종류를 다른 것으로 바꾸고, 적용 버튼을 클릭했을 때
* 패치 후

#### SNR#1776 소명 요청 화면에서 임직원 선택 창을 열었다 닫은 후 다시 열면 부서 트리가 제대로 표시되지 않는 문제 해결

소명 요청 화면에서 소명 대상자나 검토자 선택 모달에 들어가서 임직원 선택 후 모달을 나갔다가 다시 들어가면 조직 트리에서 기존에 선택한 임직원의 부서만 표시되고 나머지 부서는 표시되지 않던 문제를 해결했습니다.

#### SNR#1818 티켓의 첨부 파일 다운로드가 첫 시도 이후 다시 시도하면 '실패' 라고 표시되는 현상

#### SNR#1826 접속 프로파일 수정/삭제 시 기존 접속 프로파일 설정이 없는 경우의 NullPointerException 오류 발생 해결

접속 프로파일 수정/삭제 시 기존 접속 프로파일 설정이 없어서 프로파일 동기화 중 발생하는 NullPointerException 오류를 해결하였습니다.

* 접속 프로파일 수정 시 NullPointerException 오류 로그

[2023-05-18 15:28:30,345] ERROR (PolicyLoaderImpl) - sonar node: policy sync failure - id=1305, module=profile, action=update, params={configs={password=null, port=21, update\_keys=[], host=192.168.56.1, entry\_type=null, user=null, use\_extended\_pasv=false, timeout=30, active\_mode=false}, code=test, protected\_configs=[password], name=test, description=, type=ftp, iv=bc9gBAuB4Z0wcxPrTnWiPg==}, created=2023-05-18 15:28java.lang.NullPointerException at com.logpresso.sonar.node.impl.ProfileSyncerImpl.\_\_M\_sync(ProfileSyncerImpl.java:100) at com.logpresso.sonar.node.impl.ProfileSyncerImpl.sync(ProfileSyncerImpl.java) at com.logpresso.sonar.node.impl.PolicyLoaderImpl.\_\_M\_dispatch(PolicyLoaderImpl.java:207) at com.logpresso.sonar.node.impl.PolicyLoaderImpl.dispatch(PolicyLoaderImpl.java) at com.logpresso.sonar.node.impl.PolicyLoaderImpl$LoaderThread.\_\_M\_runOnce(PolicyLoaderImpl.java:356) at com.logpresso.sonar.node.impl.PolicyLoaderImpl$LoaderThread.runOnce(PolicyLoaderImpl.java) at com.logpresso.sonar.node.impl.PolicyLoaderImpl$LoaderThread.\_\_M\_run(PolicyLoaderImpl.java:300) at com.logpresso.sonar.node.impl.PolicyLoaderImpl$LoaderThread.run(PolicyLoaderImpl.java)

* 접속 프로파일 삭제 시 NullPointerException 오류 로그

[2023-05-18 15:28:35,354] ERROR (PolicyLoaderImpl) - sonar node: policy sync failure - id=1307, module=profile, action=remove, params={types=[ftp], names=[test2]}, created=2023-05-18 15:28java.lang.NullPointerException at com.logpresso.sonar.node.impl.ProfileSyncerImpl.\_\_M\_sync(ProfileSyncerImpl.java:61) at com.logpresso.sonar.node.impl.ProfileSyncerImpl.sync(ProfileSyncerImpl.java) at com.logpresso.sonar.node.impl.PolicyLoaderImpl.\_\_M\_dispatch(PolicyLoaderImpl.java:207) at com.logpresso.sonar.node.impl.PolicyLoaderImpl.dispatch(PolicyLoaderImpl.java) at com.logpresso.sonar.node.impl.PolicyLoaderImpl$LoaderThread.\_\_M\_runOnce(PolicyLoaderImpl.java:356) at com.logpresso.sonar.node.impl.PolicyLoaderImpl$LoaderThread.runOnce(PolicyLoaderImpl.java) at com.logpresso.sonar.node.impl.PolicyLoaderImpl$LoaderThread.\_\_M\_run(PolicyLoaderImpl.java:300) at com.logpresso.sonar.node.impl.PolicyLoaderImpl$LoaderThread.run(PolicyLoaderImpl.java)

#### SNR#1841 이미지 파일 외에 티켓 첨부 파일 다운로드 시 로그인 화면 출력 되는 문제

#### SNR#1843 티켓 추가 화면에서 파일 첨부 시 티켓 생성에 실패하는 문제

#### SNR#1846 첨부파일에 특수문자가 있을 경우 업로드 후 업로드 중 텍스트가 변경되지 않음

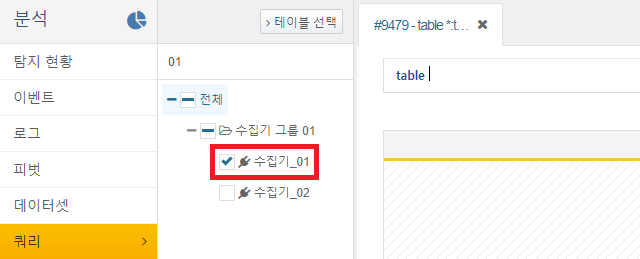
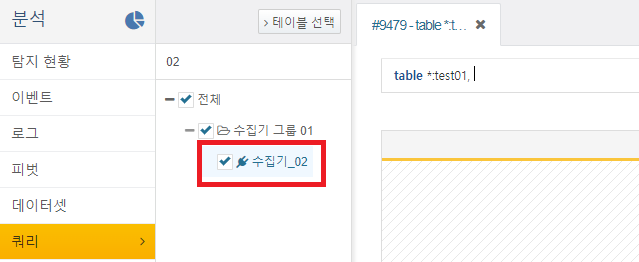
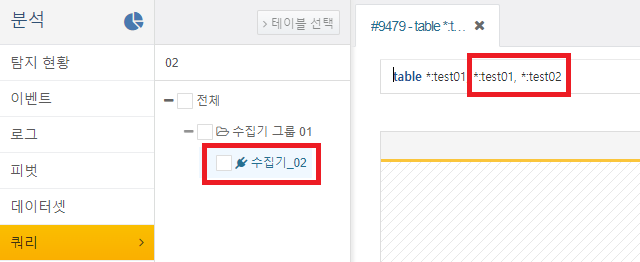
#### SNR#1851 종속 변수 수동 추가시 범례 순서가 반영되지 않는 현상

#### SNR#1882 쿼리 위젯 이름 50자 초과 입력 시 validator 동작하지 않고 생성 실패하는 현상

#### SNR#1883 쿼리 화면에서 테이블 트리 필터/체크 후, 테이블 선택된 항목이 해제되지 않는 오류 해결

분석 > 쿼리 화면에서 테이블 트리 패널에서 필터/체크 후, 테이블 선택된 항목이 해제되지 않고 다음 테이블 선택 시에도 같이 반영되던 오류가 해결되었습니다.

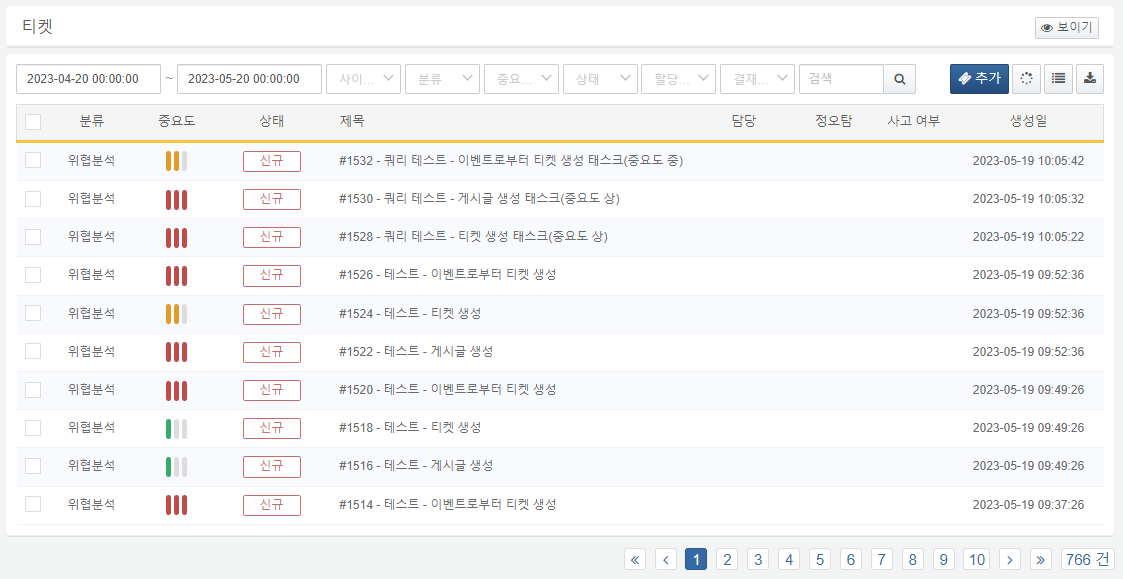
발생했던 오류는 다음 절차와 같고, 현재 선택된 테이블만 테이블 선택 시 반영되도록 수정되었습니다.

* 테이블 트리 패널에서 필터(예: 01)
* 테이블 선택 후, 체크 해제된 것으로 표시됨
* 다른 필터 적용(예: 02)
* 테이블 선택 후, 쿼리가 추가될 때 기존 필터/체크/선택된 테이블도 함께 추가되는 오류 발생

#### SNR#1913 마에스트로 티켓 생성 명령어의 중요도 설정이 되지 않는 문제 해결

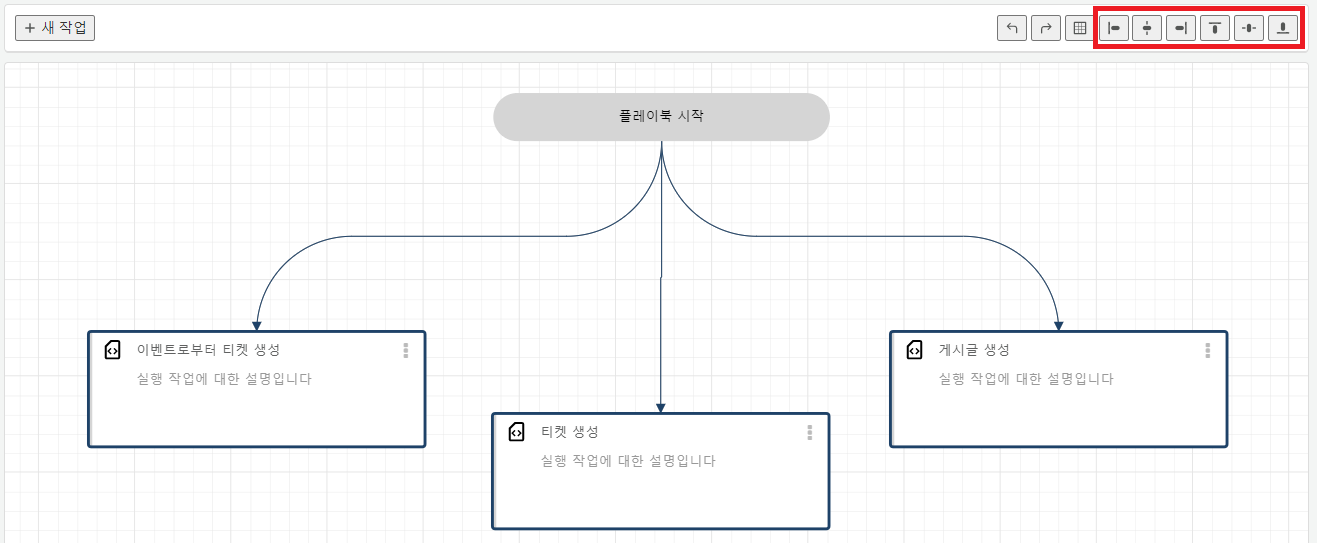
플레이북 작업에서 티켓 중요도를 설정해도 기본값인 LOW로만 설정되는 오류가 발견되어, 마에스트로 티켓 생성 명령어의 중요도 설정이 되지 않는 문제를 해결하였습니다.

* 티켓 생성 명령어
* 이벤트로부터 티켓 생성: maestro-create-ticket-from-event
* 티켓 생성: maestro-create-ticket
* 게시글 생성: maestro-create-article



#### SNR#1936 플레이북 디자이너에서 태스크 정렬 기능이 동작하지 않는 문제 해결

플레이북 디자이너에서 태스크 다중 선택(shift + 마우스 클릭/드래그) 이후, 태스크 정렬 기능이 동작하지 않는 문제를 해결하였습니다.



#### SNR#1937 머신러닝 모델에 사용 중인 학습 데이터셋 삭제 시 오류 메시지 등 보완

#### SNR#1981 탐지 현황 팝업에서 info 버튼 클릭 시 자세한 정보 보기 내용 잘림

#### SNR#1999 시나리오에서 중복 이벤트 제거를 설정한 경우, 티켓 삭제 및 완료 처리 시 NullPointerException 오류 발생 해결

해당 이슈는 로그프레소 4.0.2205.0 이상, 4.0.2303.0 이하 버전에서 발생합니다.

실시간/배치 탐지 시나리오에서 중복 이벤트 제거를 설정한 시나리오가 있는 경우, 티켓 삭제 및 완료 처리 시에 NPE(NullPointerException) 오류가 발생하는 문제를 해결하였습니다.

* 티켓 삭제 시 NullPointerException 오류 로그

[2023-05-24 09:26:58,163] WARN (TicketServiceImpl) - sonar core: ticket listener should not throw any exceptionjava.lang.NullPointerException at com.logpresso.sonar.api.impl.AlertServiceImpl$TicketCloseHandler.\_\_M\_getMatchingKeys(AlertServiceImpl.java:840) at com.logpresso.sonar.api.impl.AlertServiceImpl$TicketCloseHandler.getMatchingKeys(AlertServiceImpl.java) at com.logpresso.sonar.api.impl.AlertServiceImpl$TicketCloseHandler.\_\_M\_removeContext(AlertServiceImpl.java:851) at com.logpresso.sonar.api.impl.AlertServiceImpl$TicketCloseHandler.removeContext(AlertServiceImpl.java) at com.logpresso.sonar.api.impl.AlertServiceImpl$TicketCloseHandler.\_\_M\_onRemove(AlertServiceImpl.java:831) at com.logpresso.sonar.api.impl.AlertServiceImpl$TicketCloseHandler.onRemove(AlertServiceImpl.java) at com.logpresso.sonar.api.impl.TicketServiceImpl.\_\_M\_removeTickets(TicketServiceImpl.java:990) at com.logpresso.sonar.api.impl.TicketServiceImpl.removeTickets(TicketServiceImpl.java) at com.logpresso.sonar.msgbus.TicketPlugin.\_\_M\_removeTickets(TicketPlugin.java:1070) at com.logpresso.sonar.msgbus.TicketPlugin.removeTickets(TicketPlugin.java) at java.base/jdk.internal.reflect.NativeMethodAccessorImpl.invoke0(Native Method) at java.base/jdk.internal.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:62) at java.base/jdk.internal.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43) at java.base/java.lang.reflect.Method.invoke(Method.java:566) at org.araqne.msgbus.handler.MsgbusPluginHandler.\_\_M\_handleMessage(MsgbusPluginHandler.java: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)

* 티켓 완료 시 NullPointerException 오류 로그

[2023-05-24 09:26:51,684] WARN (TicketServiceImpl) - sonar core: ticket listener should not throw any exceptionjava.lang.NullPointerException at com.logpresso.sonar.api.impl.AlertServiceImpl$TicketCloseHandler.\_\_M\_getMatchingKeys(AlertServiceImpl.java:840) at com.logpresso.sonar.api.impl.AlertServiceImpl$TicketCloseHandler.getMatchingKeys(AlertServiceImpl.java) at com.logpresso.sonar.api.impl.AlertServiceImpl$TicketCloseHandler.\_\_M\_removeContext(AlertServiceImpl.java:851) at com.logpresso.sonar.api.impl.AlertServiceImpl$TicketCloseHandler.removeContext(AlertServiceImpl.java) at com.logpresso.sonar.api.impl.AlertServiceImpl$TicketCloseHandler.\_\_M\_onClose(AlertServiceImpl.java:826) at com.logpresso.sonar.api.impl.AlertServiceImpl$TicketCloseHandler.onClose(AlertServiceImpl.java) at com.logpresso.sonar.api.impl.TicketServiceImpl.\_\_M\_closeTicket(TicketServiceImpl.java:942) at com.logpresso.sonar.api.impl.TicketServiceImpl.closeTicket(TicketServiceImpl.java) at com.logpresso.sonar.msgbus.TicketPlugin.\_\_M\_closeTickets(TicketPlugin.java:1049) at com.logpresso.sonar.msgbus.TicketPlugin.closeTickets(TicketPlugin.java) at java.base/jdk.internal.reflect.NativeMethodAccessorImpl.invoke0(Native Method) at java.base/jdk.internal.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:62) at java.base/jdk.internal.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43) at java.base/java.lang.reflect.Method.invoke(Method.java:566) at org.araqne.msgbus.handler.MsgbusPluginHandler.\_\_M\_handleMessage(MsgbusPluginHandler.java: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)

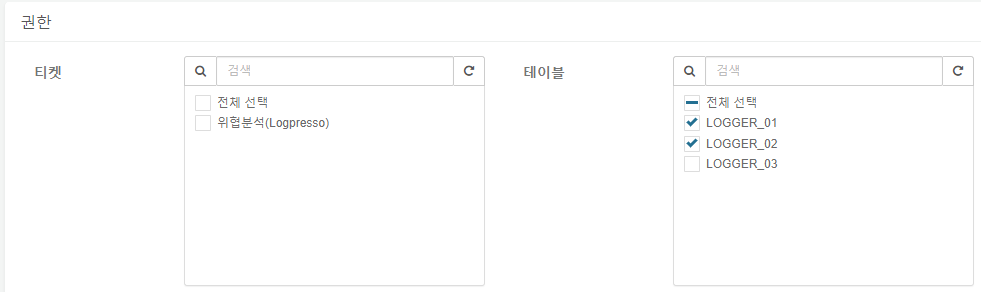
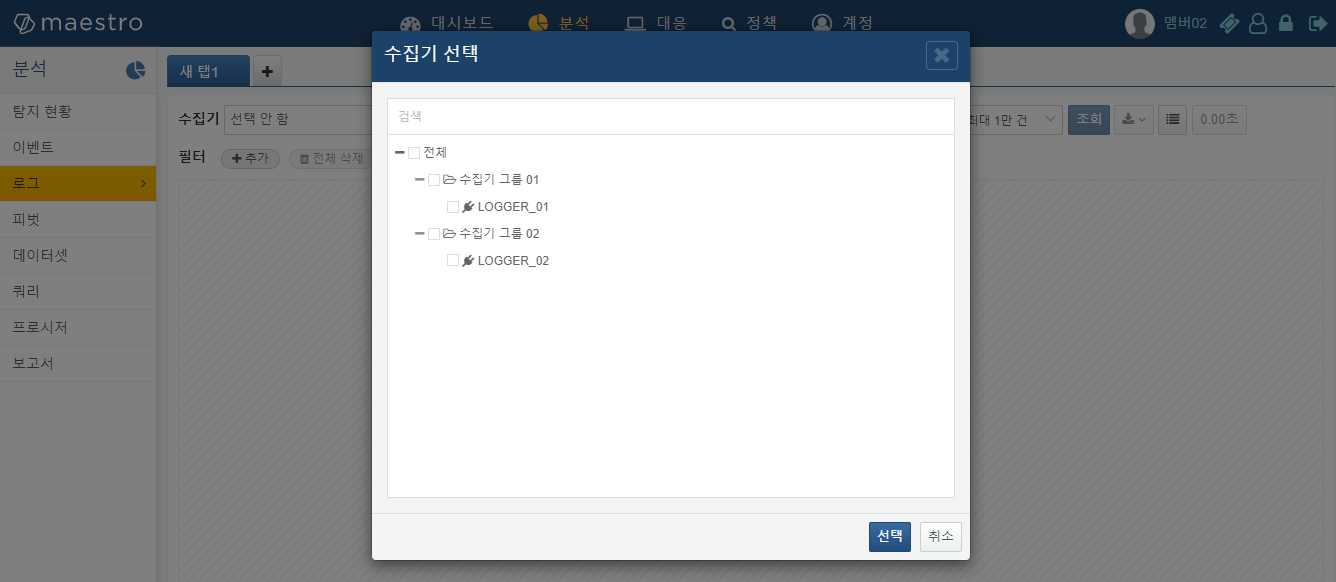
#### SNR#2022 티켓 축약 0초 설정 시 100ms 범위 내 생성된 티켓이 축약되는 문제

#### SNR#2023 보고서 서식 목록 다운로드시 현재 페이지만 다운로드 되는 오류

#### SNR#2031 수집기 선택 트리에서 테이블 조회 권한이 없는 수집기가 표시되는 문제 해결

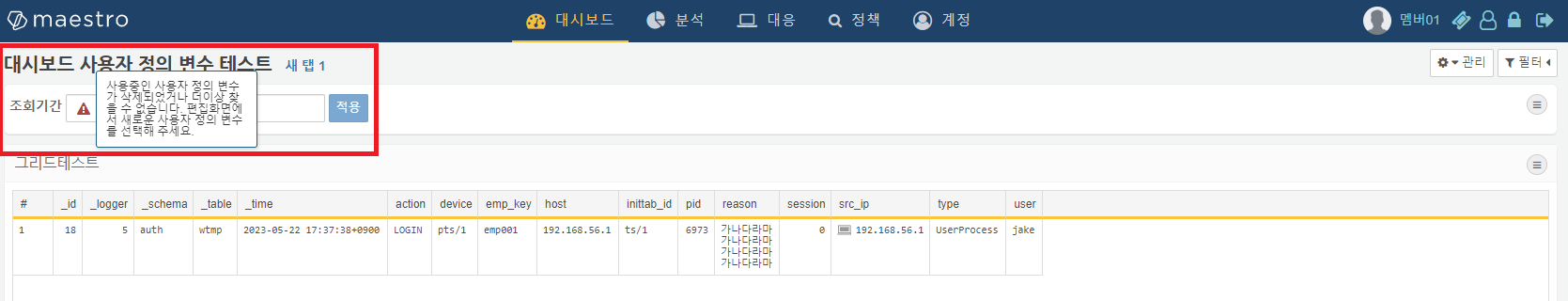
수집기 선택 트리에서 테이블 조회 권한이 없는 수집기가 표시되는 문제를 해결하였습니다.

사용자 권한 계정만 해당되며, 관리자 이상 계정에서는 모든 수집기가 표시됩니다.

* 대상 화면
* 대시보드 > 윗젯 > 쿼리 위젯
* 분석 > 이벤트
* 분석 > 로그
* 분석 > 피벗
* 분석 > 쿼리
* 테이블 조회 권한 설정에 따른 수집기 선택 트리
* 테이블 조회 권한
* 수집기 선택 트리

#### SNR#2043 사용자 정의 변수를 사용하는 대시보드를 공유하였을 때, 사용자 계정에서 입력 컨트롤을 사용할 수 없는 문제 해결

사용자 정의 변수를 사용하는 입력 컨트롤이 포함된 대시보드를 공유하였을 때, 사용자 계정에서 사용자 정의 변수 조회 권한이 없어서 입력 컨트롤을 사용할 수 없는 문제를 해결하였습니다.

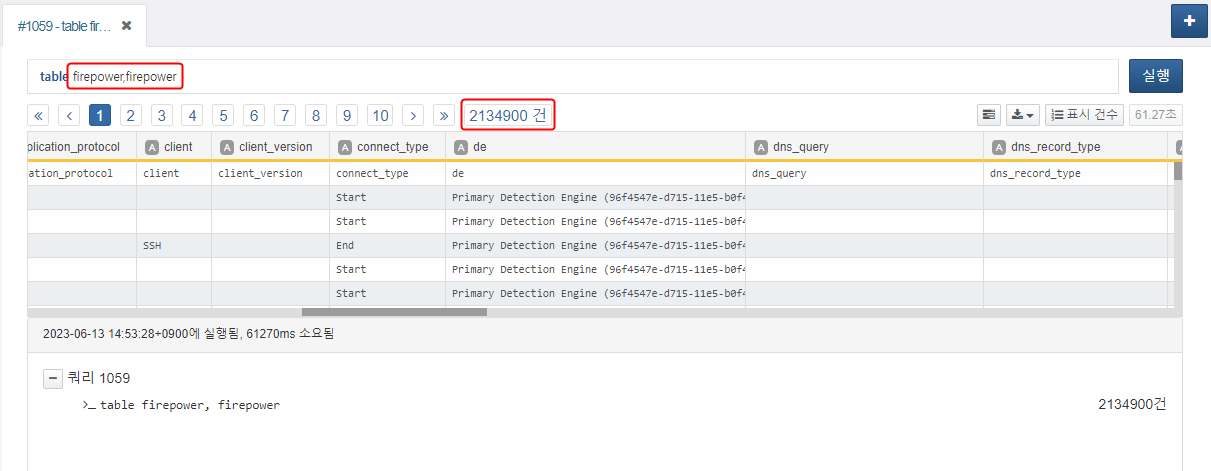
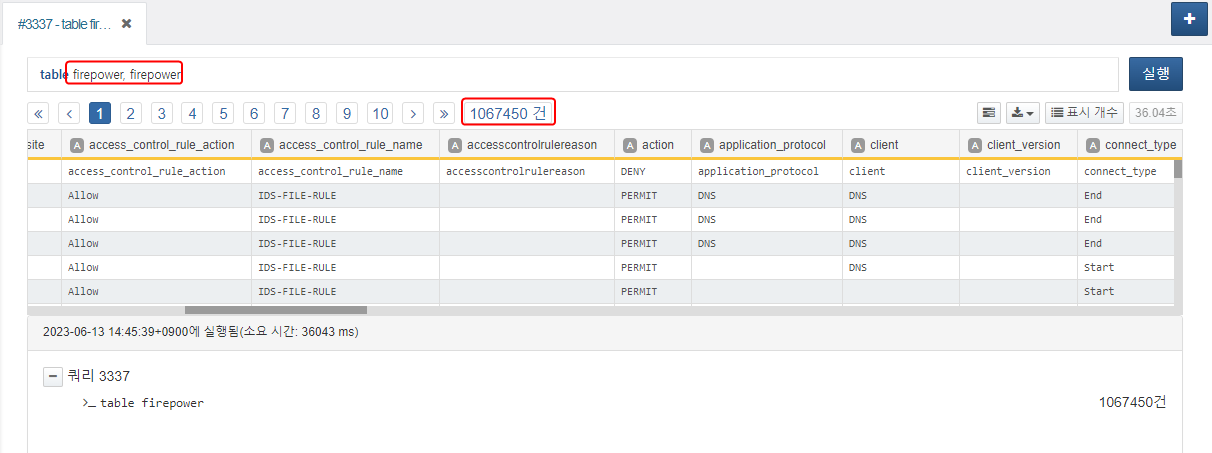
* 패치 전 오류 화면: 사용자 정의 변수 조회 권한이 없어서 입력 컨트롤 사용 불가
* 패치 후: 사용자 계정에서도 정상적으로 입력 컨트롤 사용 가능
* 사용자 정의 변수 권한 정책

|  |  |  |  |
| --- | --- | --- | --- |
| 권한 코드 | 권한 이름 | 사용자 정의 변수 | 사용자 계정 권한 보유 |
| DASHBOARD\_ADMIN | 대시보드 관리 | 조회/추가/수정/삭제 | X |
| DASHBOARD\_EDIT | 대시보드 편집 | 조회 | O |
| DASHBOARD\_VIEW | 대시보드 조회 | 조회 | O |
| DASHBOARD\_WIDGET\_EDIT | 위젯 편집 | 조회/추가/수정/삭제 | O |
| DASHBOARD\_WIDGET\_VIEW | 위젯 조회 | 조회 | O |

* 사용자 정의 변수 권한에 영향을 받는 기능: 대시보드 입력 컨트롤, 피벗 동적 필터
* 관리자 이상 계정은 모든 권한을 가집니다.
* 사용자 계정은 기본적으로 대시보드 및 위젯 편집/조회 권한을 가지므로 사용자 정의 변수(소유자 여부 무관)에 대한 조회/추가/수정/삭제 권한을 가집니다.
* 별도 역할(role)을 정의한 경우는 위 권한에 따라 사용자 정의 변수 권한을 가집니다.
* 위 권한 모두가 없는 경우, 사용자 정의 변수를 사용할 수 없습니다.
* 대시보드: 사용자 정의 변수를 포함한 입력 컨트롤 사용 불가
* 피벗 화면: 동적 필터 사용 불가(조회 및 시간 단위 절사는 사용 가능)

#### SNR#2050 table, fulltext 커맨드에 대상 테이블 중복 지정 시 동일 레코드가 반복 출력되는 문제 해결

table, fulltext 커맨드의 조회 대상을 중복하여 입력하는 경우, 결과가 반복 출력되는 문제를 해결하였습니다.

* 패치 전: 조회 대상을 중복 입력하는 경우, 결과가 반복 출력
* 패치 후: 조회 대상을 중복 입력하는 경우에도 결과가 한번만 출력

#### SNR#2062 티켓으로부터 비롯된 플레이북 조회가 느린 문제, 티켓 정오탐/사고 관련 권한이 클러스터 관리자에게만 부여된 문제 해결

#### SNR#2064 분석 노드에서 테이블 삭제 시 수집 노드에서 테이블 데이터 파일이 삭제되지 않고 남아있는 문제 해결

분석 노드에서 테이블을 삭제할 경우 분석 노드에 존재하는 테이블 데이터는 정상 삭제되지만 수집 노드에서는 테이블 데이터가 디스크에 여전히 남아있던 문제를 해결했습니다.

#### SNR#2073 fulltext 쿼리 명령어의 중첩된 부등호 연산 정합성 문제 해결

블룸필터가 적용된 인덱스를 대상으로 fulltext 쿼리를 수행할 때 검색 조건에 동일한 필드에 대해 동일 부등호 연산을 'or' 문으로 묶을 경우 검색 결과가 일부 누락되는 문제를 해결했습니다.

**기존 버전에서 정합성이 맞지 않던 쿼리문 예시**

* src\_ip 필드에 대해 '<' 연산을 수행하는 조건 2개가 'or' 문으로 묶임
* fulltext src\_ip < ip("220.0.0.0") or src\_ip < ip("221.0.0.0") from zc0 | stats count as fulltext\_count

#### SNR#2085 ldapsearch 쿼리 명령어에서 1,000건 결과 제한으로 실패하는 오류 해결

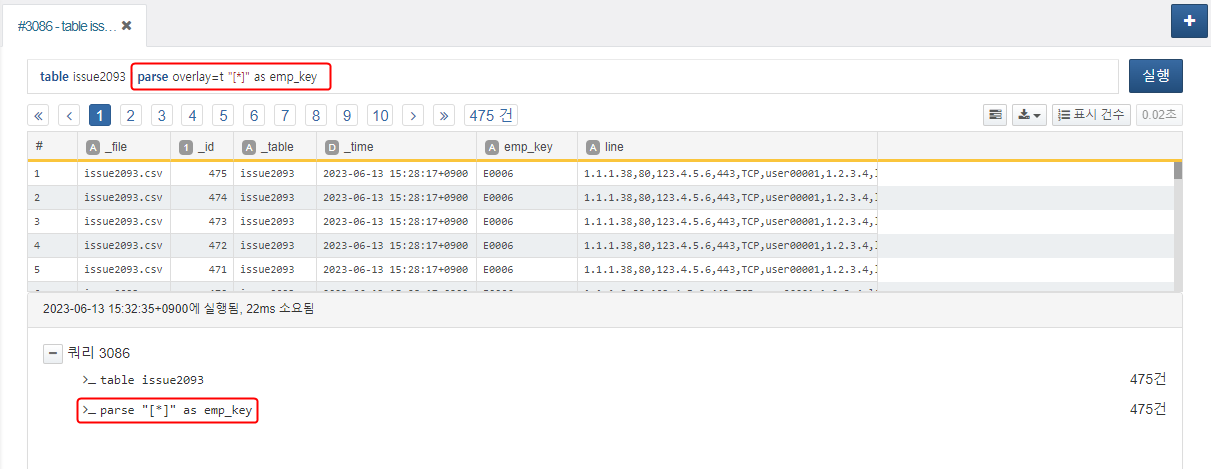
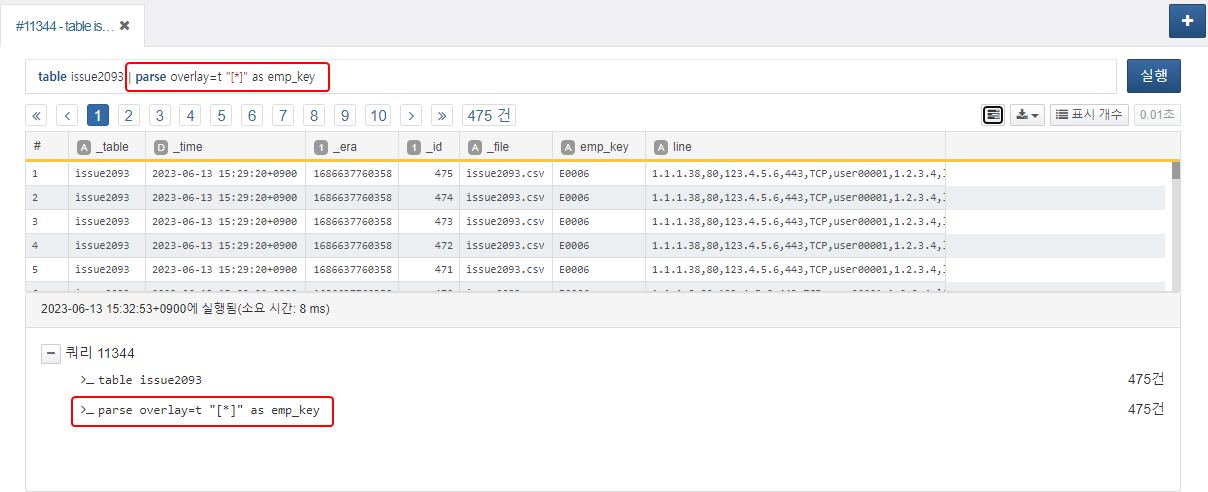
ldapsearch 쿼리 명령어에서 1,000건 결과 제한으로 실패하는 오류를 해결하였습니다.

* 오류 로그

araqne logdb: query [89556] task [query: 39556 scan: Idapsearch profile=1dap] failedjava.lang.illegalStateException: LDAPException: sizelimit Exceeded (4) Sizelimit ExceededLDAPException: Matched DN: at org.logpresso.ldap.impl.LdapSearchCommand.run(LdapSearchCommand.java:92)

#### SNR#2093 parse 커맨드 실행 계획 출력 시 overlay 옵션이 누락되는 현상 해결

parse 커맨드의 실행 계획 출력 시 overlay 옵션이 누락되는 현상을 해결하었습니다.

* 패치 전: parse 커맨드의 overlay 옵션 누락
* 패치 후: parse 커맨드의 overlay 옵션 적용

#### SNR#2094 센트리 Linux Account Watcher 수집기 로케일 적용 오류 수정

#### SNR#2095 SNMP 수집기 설정에 잘못된 oid 필드 매핑 값을 입력했을 때 오류 처리 추가

SNMP 수집기를 생성/수정할 때 'oid 필드 매핑 목록' 항목에 입력한 설정 값에 오류가 있으면 수집기를 생성/수정하지 않도록 변경했습니다.

* oid 필드 매핑의 잘못된 예
* oid 혹은 필드만 입력
* 'oid='만 입력하고 필드 누락
* '=필드' 형태로 입력하고 oid 누락

#### SNR#2103 특정 쿼리 커맨드에서 쿼리에 매개변수 사용 불가능한 문제 해결

textfile, csvfile, xmlfile, jsonfile 커맨드들은 파일 경로를 파라미터로 받아 파일을 출력하는 드라이버 쿼리 커맨드입니다.이 파일 경로를 매개변수로 지정했을 때 쿼리 유효성 검사에 실패해 쿼리 생성이 실패하는 문제가 수정되었습니다.

사용 예시

set path="log/araqne.log" | textfile $("path")

#### SNR#2104 인덱스 동시 접근 시 인덱스 토크나이저가 누수되는 문제 해결

하나의 인덱스에 비동기 스트림 쿼리 등으로 여러 작업이 동시에 접근할 때 토크나이저 풀에 할당된 토크나이저가 정리되지 않고 누수되는 문제를 해결했습니다.

인덱스 객체가 더 이상 사용하지 않는 메모리를 회수하는 logpresso.triggerOnlineIndexGC 로그프레소 셸 명령어를 추가했습니다. logpresso.triggerOnlineIndexGC 명령어의 문법은 다음과 같습니다.

logpresso.triggerOnlineIndexGC [tablepattern]

**tablepattern**

가비지 컬렉션 대상이 되는 테이블 이름의 문자열 패턴. 와일드카드(\*)를 지원합니다.

#### SNR#2108 SNMP 수집 버그 수정

#### SNR#2127 쿼리 종료 대기로 인한 셧다운 hang

#### SNR#2145 라이선스 주입 시 버전 4 인식 실패