## 릴리스 4.0.2502.0

araqne-core 버전이 4.0.3으로 업데이트되었습니다.

4.0.2502.0 초기 배포 버전에서 심각한 메모리 누수 현상이 발견되었습니다. 2025-03-13 15:19:00 시점 이전 패키지(빌드 번호 3084)를 받으신 분들은 수정된 배포 패키지(빌드번호 3085)를 적용해주시기 바랍니다.

마리아디비 버전이 10.5 미만일 경우 설치나 패치에 실패하는 이슈가 있습니다. 다음 패치를 기다리시거나 SNR#2689 이슈 릴리스 노트에 나온 우회 방법으로 패치를 진행하시길 바랍니다.

### 메인 피쳐

|  |  |
| --- | --- |
| 식별자 | 항목 |
| [SNR#2660](https://docs.logpresso.comnull) | 로그 스키마 용어사전 기능 추가 |
| [SNR#2689](https://docs.logpresso.comnull) | 이메일 MFA 기능 추가 |

### 신규 기능

|  |  |
| --- | --- |
| 식별자 | 항목 |
| [SNR#2589](https://docs.logpresso.comnull) | 위협 인텔리전스 조회, 활성화, 비활성화 REST API 추가 |
| [SNR#2631](https://docs.logpresso.comnull) | 주소 그룹 대용량 업로드 기능 추가 |
| [SNR#2846](https://docs.logpresso.comnull) | 로그프레소 런처 배포 |

### 기능 개선

|  |  |
| --- | --- |
| 식별자 | 항목 |
| [SNR#2527](https://docs.logpresso.comnull) | SNMP 트랩 수집기 설정에서 접속 프로파일 드롭다운 선택 기능 추가 |
| [SNR#2530](https://docs.logpresso.comnull) | 접속 프로파일의 접속 상태를 확인할 수 있는 기능 추가 |
| [SNR#2538](https://docs.logpresso.comnull) | 스토리지 인증서 동기화 기능 추가 및 테이블 암호화 설정 방법 변경 |
| [SNR#2547](https://docs.logpresso.comnull) | 라이선스 경고 표시 기능 추가 |
| [SNR#2565](https://docs.logpresso.comnull) | 수집기 목록 조회 성능 개선 |
| [SNR#2599](https://docs.logpresso.comnull) | 쿼리 REST API 출력 type에 단일 JSON 파일 유형 추가 |
| [SNR#2604](https://docs.logpresso.comnull) | 소명 상세 근거 항목에 URL 필드가 존재하면 하이퍼링크로 변환하는 기능 추가 |
| [SNR#2621](https://docs.logpresso.comnull) | 전달 서버 데이터 전송 로직 개선 및 스왑 용량 확인 쿼리 명령어 추가 |
| [SNR#2657](https://docs.logpresso.comnull) | 로그 스키마 검색 기능 추가 |
| [SNR#2658](https://docs.logpresso.comnull) | 시나리오 목록 화면에 소명/티켓 사용 여부 표시 칼럼 추가 |
| [SNR#2666](https://docs.logpresso.comnull) | 센트리 자동 설치 시 사용자가 지정한 스크립트 사용 지원 |
| [SNR#2674](https://docs.logpresso.comnull) | 수집기 생성 시 암호화한 테이블을 생성하는 기능 추가 및 기존 테이블 암호화 여부 표시 기능 추가 |
| [SNR#2722](https://docs.logpresso.comnull) | ISAC 위협 인텔리전스 피드 제거 |
| [SNR#2740](https://docs.logpresso.comnull) | 티켓 태그 색상 입력 방식 개선 |
| [SNR#2741](https://docs.logpresso.comnull) | 수집기 화면 너비 확대 |
| [SNR#2753](https://docs.logpresso.comnull) | 배치 시나리오 실행 시 테이블 적재가 지연될 때 티켓 근거자료가 보이지 않는 문제 해결 |
| [SNR#2756](https://docs.logpresso.comnull) | 소명 템플릿 매크로에 소명 생성일 추가 |
| [SNR#2764](https://docs.logpresso.comnull) | SNMP 트랩 로그 개선 |
| [SNR#2765](https://docs.logpresso.comnull) | 생명주기 프로파일 생성 및 수정 시 직접 복사 옵션 추가 |
| [SNR#2773](https://docs.logpresso.comnull) | 소나 메일 설정에 프록시 설정 추가 |
| [SNR#2792](https://docs.logpresso.comnull) | 예약된 쿼리 쿼리문 10,000자까지 지원 |
| [SNR#2812](https://docs.logpresso.comnull) | 계정 추가 시 임직원 연결 기능 삭제 |

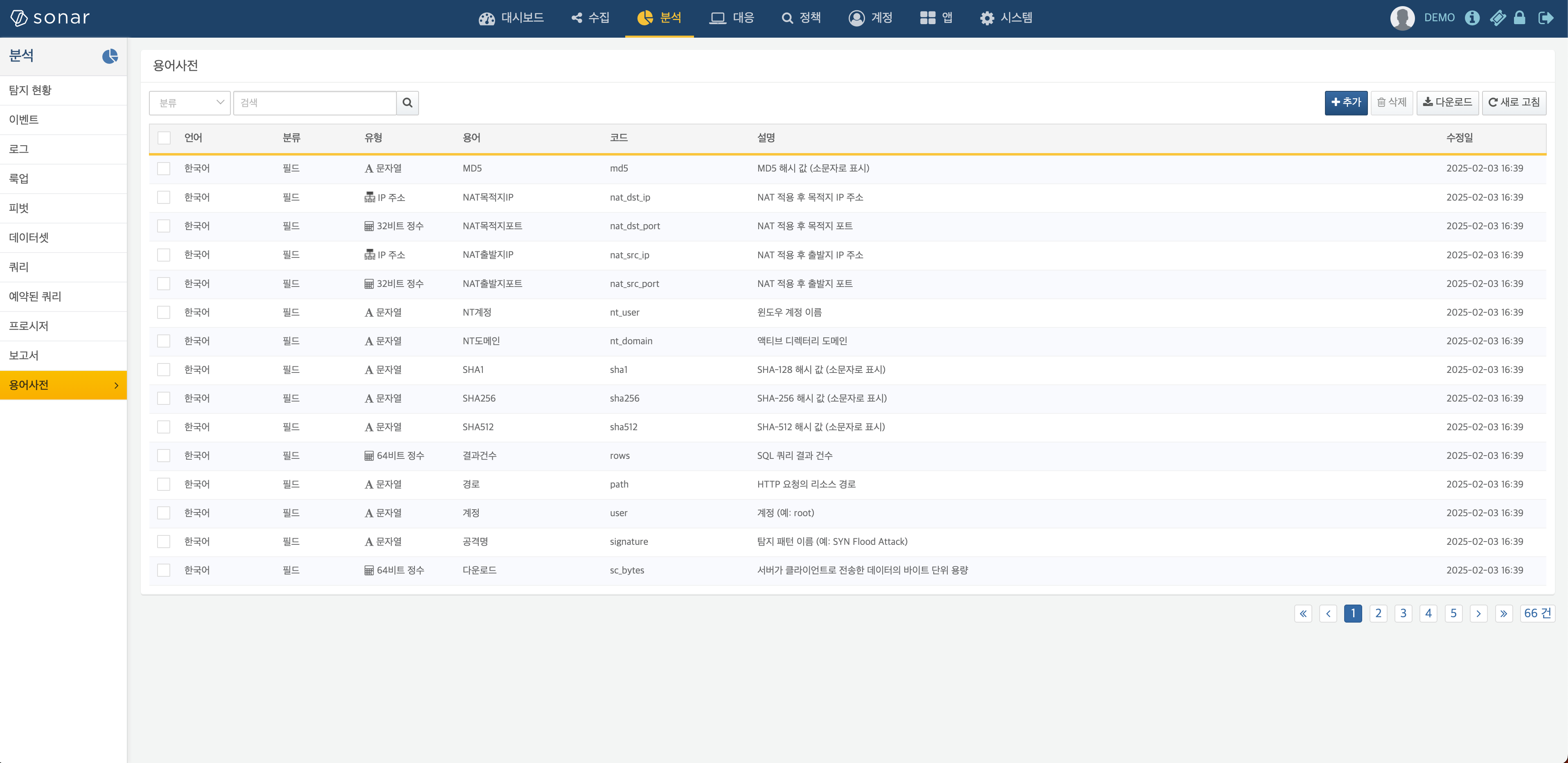
### 버그 해결

|  |  |
| --- | --- |
| 식별자 | 항목 |
| [SNR#2598](https://docs.logpresso.comnull) | 윈도우 이벤트 수집기가 이벤트 XML 파싱을 실패할 때 간헐적으로 중단되는 문제 해결 |
| [SNR#2725](https://docs.logpresso.comnull) | REST API IP 접근 제어 시 로드밸런서 구성 지원 |
| [SNR#2727](https://docs.logpresso.comnull) | sonar-set-ip-address 쿼리 명령어 사용 시 동일 IP가 추가되는 문제 해결 |
| [SNR#2731](https://docs.logpresso.comnull) | 일부 메일 클라이언트에서 메일 발신자 이름이 정상적으로 표기되지 않는 문제 해결 |
| [SNR#2745](https://docs.logpresso.comnull) | string() 함수 사용시 날짜 지시자 형식이 잘못된 경우 NPE 오류 발생 해결 |
| [SNR#2748](https://docs.logpresso.comnull) | null 값만 존재하는 필드에 대해 dc() 집계 함수 수행 시 결과가 0이 아닌 null이 나오던 문제 해결 |
| [SNR#2755](https://docs.logpresso.comnull) | 소명 근거자료 탭 정렬 시 미분류와 기타 탭이 제일 마지막 순서로 오도록 수정 |
| [SNR#2760](https://docs.logpresso.comnull) | 시나리오에서 소명 설정시 소나 계정이 없는 2차 검토자가 목록에 표시되는 문제 해결 |
| [SNR#2769](https://docs.logpresso.comnull) | 라이선스 연동 시 서버 타임존이 안맞는 경우 invalid-hash-code 오류 발생 해결 |
| [SNR#2799](https://docs.logpresso.comnull) | 8192 바이트보다 큰 수집모델을 불러올 수 없는 문제 해결 |

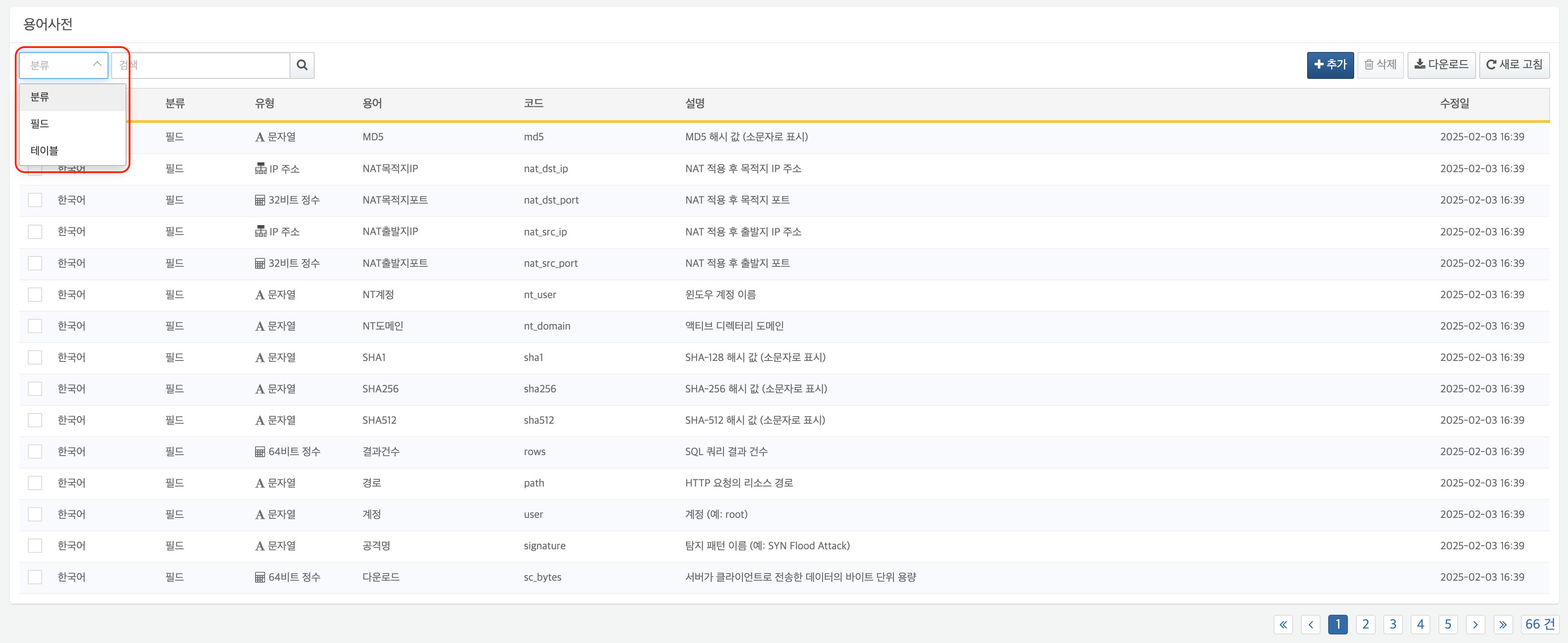
### 상세 내역

#### SNR#2660 로그 스키마 용어사전 기능 추가

로그 스키마에서 사용하는 필드 목록을 취합해서 검색할 수 있는 기능인 용어사전을 추가했습니다. 패키지 업데이트를 하면 용어사전 메뉴에 기본으로 내장된 용어들을 확인할 수 있습니다.



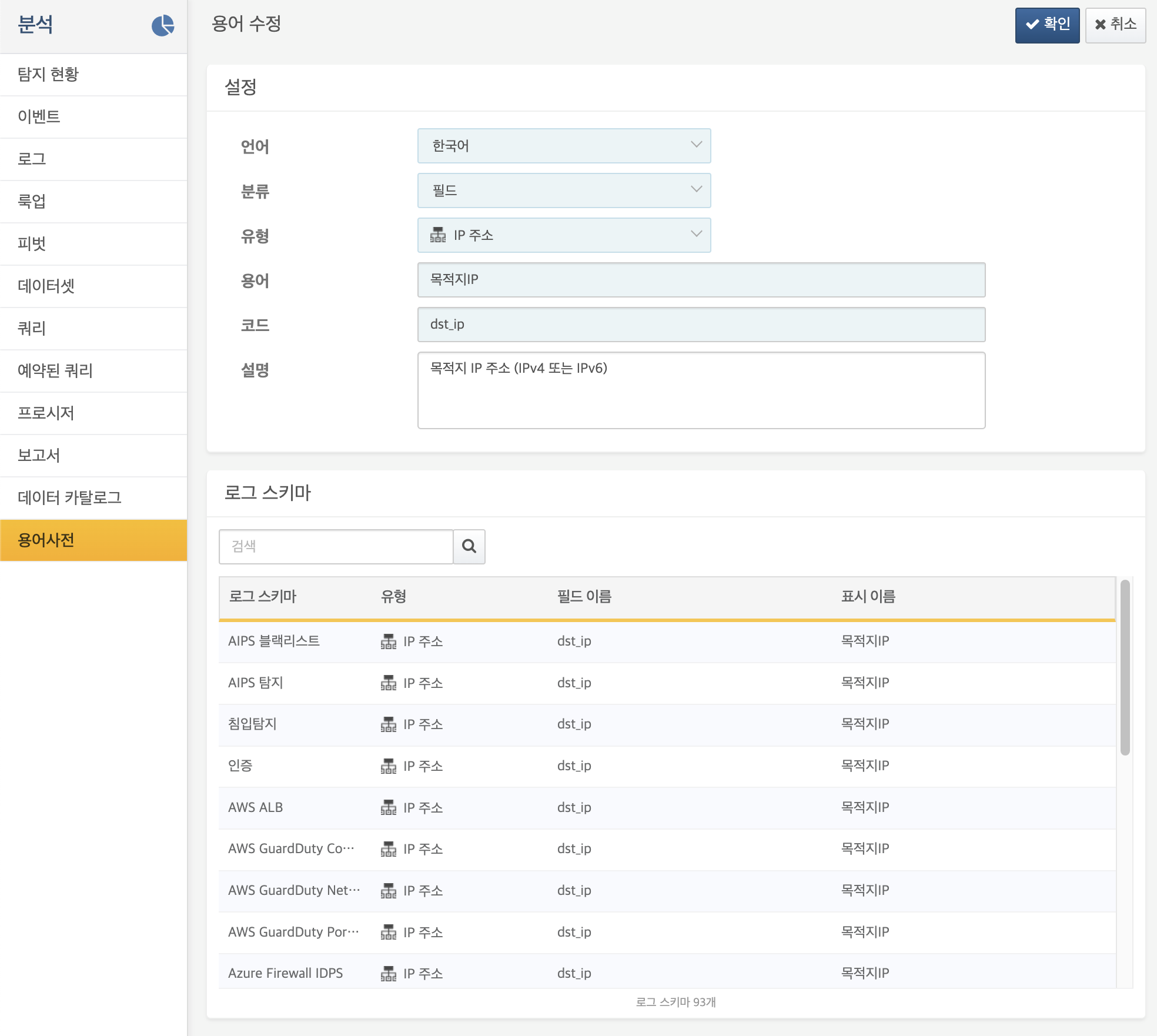
용어는 필드 용어와 테이블 용어로 구분되며, 내부에서 사용하는 코드와 그 의미를 관리할 수 있습니다. 필드 용어의 경우 로그 스키마에서 사용하는 필드의 이름과 의미를 관리합니다. 테이블 용어의 경우 테이블 이름 규칙(컨벤션)을 관리할 수 있습니다.



로그 스키마 작성 시 등록된 용어를 바탕으로 필드 이름 또는 표시 이름 자동 완성 기능도 지원합니다. 로그 스키마에서 사용하고 있는 유사한 필드 이름과 표시 이름도 보여줍니다.



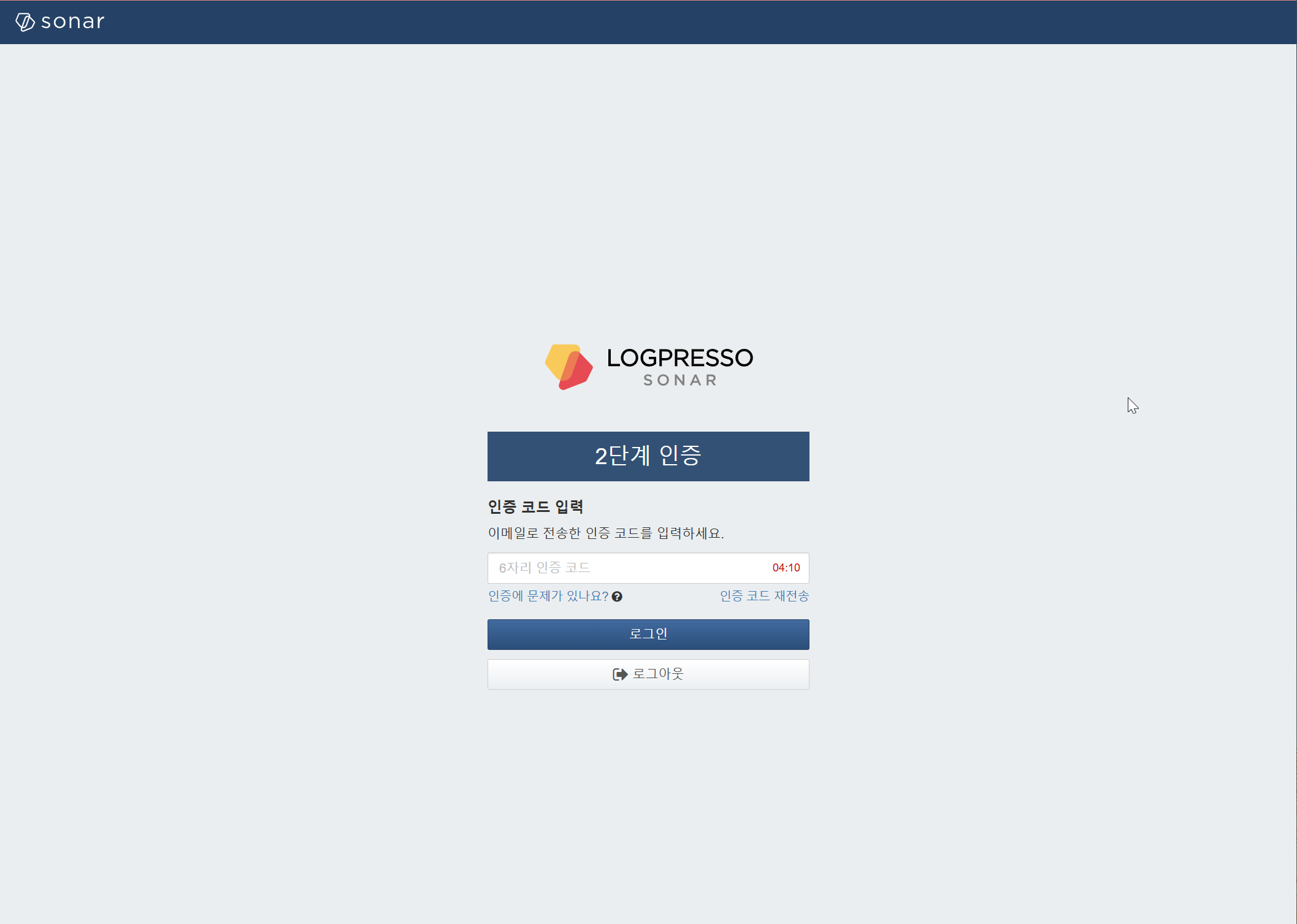
각 용어를 클릭하면 해당 필드 이름을 포함하는 모든 로그 스키마 목록을 표시합니다.



#### SNR#2689 이메일 MFA 기능 추가

로그프레소 소나 로그인 MFA 인증 방식에 이메일 유형이 추가되었습니다.

이메일 MFA 인증 기능을 설정한 경우, 로그인 시 인증 코드 입력 화면이 보입니다.

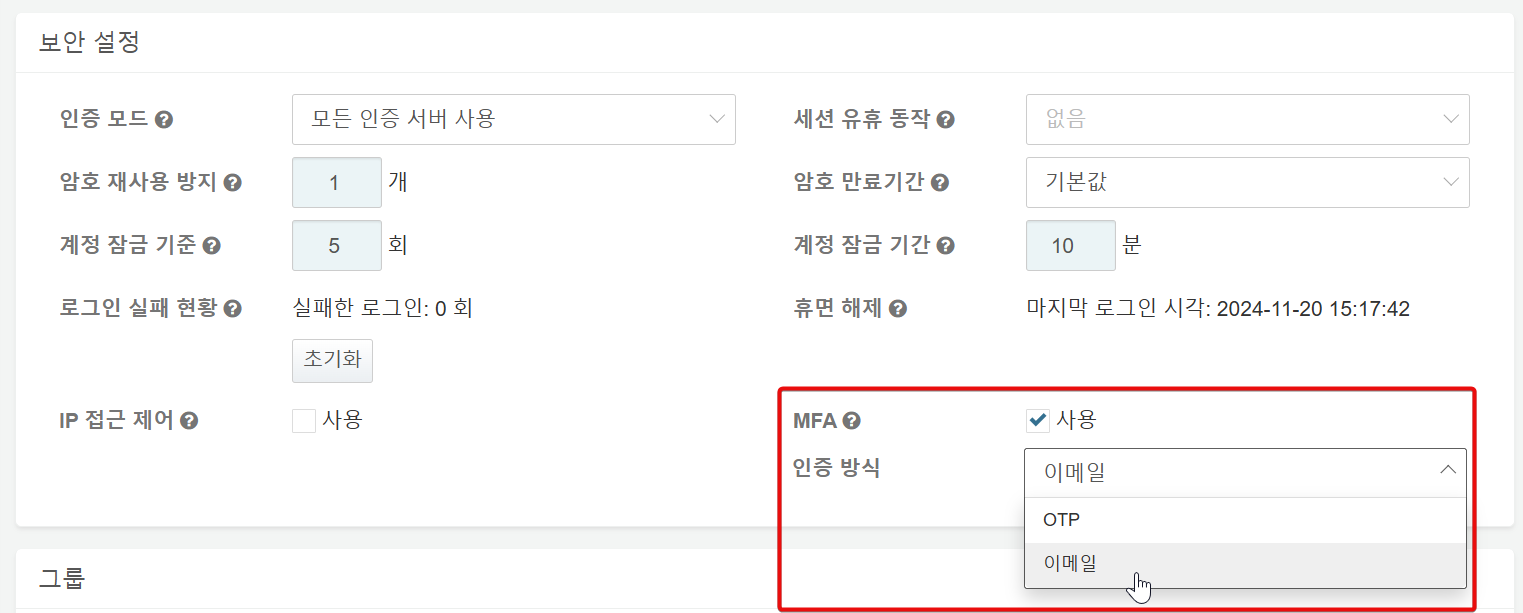


이메일을 확인하여 인증 코드를 가져올 수 있습니다.



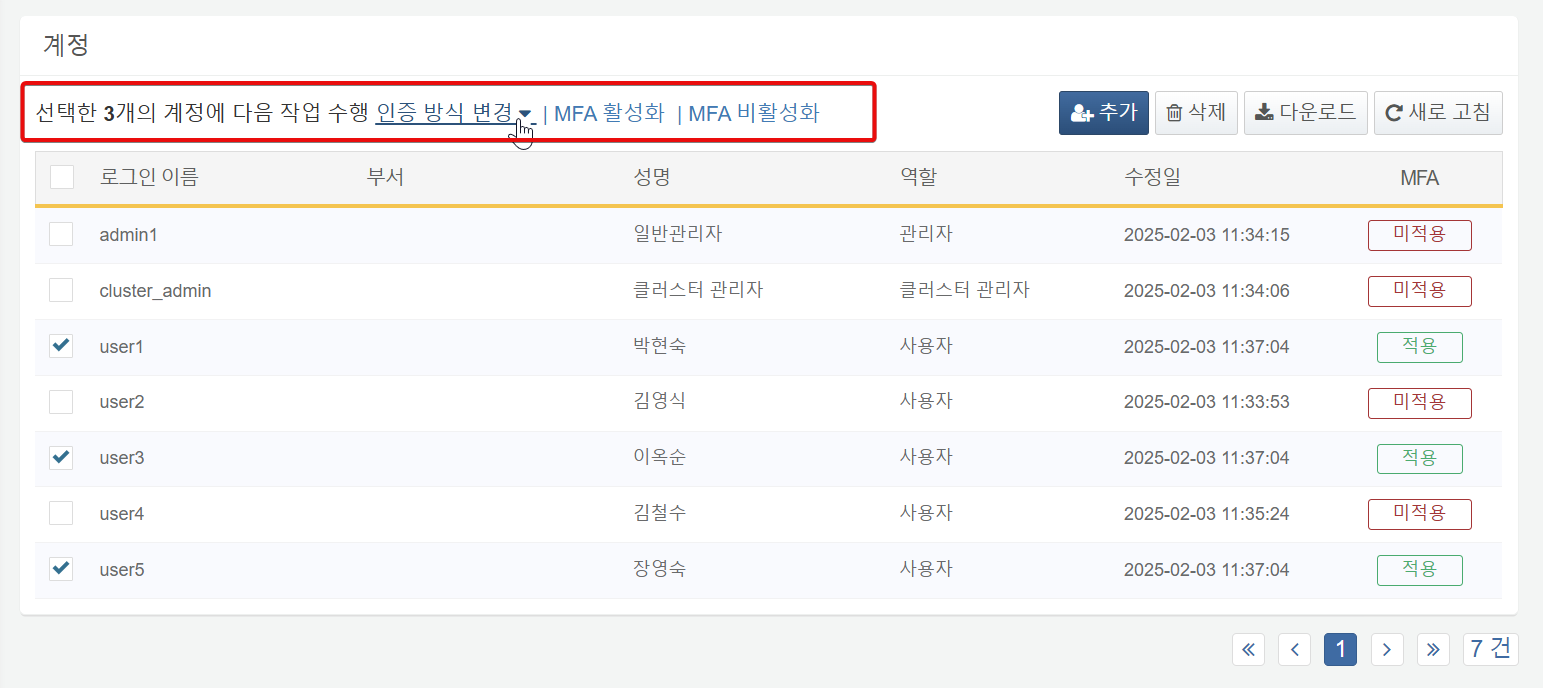
개별 계정에 대해 MFA 인증 방식을 선택하려면 계정 추가 혹은 편집 화면의 MFA 설정에서 OTP와 이메일 중에 하나를 선택합니다.

* **OTP:** OTP 방식(기본값, 기존 2FA 설정과 동일)
* **메일:** 계정에 설정된 이메일 주소로 메일 인증 코드를 보내 인증하는 방식



여러 계정에 대해 인증 방식을 일괄 변경하려면 다음 방법을 사용합니다.

* 인증 방식 변경: 선택한 계정들의 MFA 설정을 OTP, 이메일 중 선택하여 적용할 수 있습니다.
* MFA 활성화: 선택한 계정들의 MFA 설정을 사용으로 변경합니다. 비활성화 전 설정된 값으로 다시 활성화됩니다.
* MFA 비활성화: 선택한 계정들의 MFA 설정을 사용 안 함으로 변경합니다.



만약 마리아디비 버전이 10.5 미만 버전을 사용하는 경우 다음 절차를 따라 설치 혹은 패치를 진행하시길 바랍니다.

로그프레소 셸에서 마이그레이션을 234번까지 수행 - 로그프레소 셸에서 다음 명령어 수행

> sonar.migrate 234

마리아디비 sonar 데이터베이스에서 다음 SQL 쿼리문을 순서대로 수행 ()

ALTER TABLE `sonar\_logos` ADD COLUMN IF NOT EXISTS `mail\_header\_logo` mediumtext DEFAULT NULL COMMENT 'base64 PNG 이미지' AFTER `login\_logo`; ALTER TABLE `sonar\_logos` ADD COLUMN IF NOT EXISTS `mail\_footer\_logo` mediumtext DEFAULT NULL COMMENT 'base64 PNG 이미지' AFTER `mail\_header\_logo`; INSERT INTO `sonar\_logos` (`host`, `mail\_header\_logo`, `mail\_footer\_logo`) (SELECT NULL, "", "" FROM DUAL WHERE NOT EXISTS (SELECT \* FROM `sonar\_logos` WHERE `host` IS NULL)); UPDATE `sonar\_logos` SET `mail\_header\_logo`="", `mail\_footer\_logo`="" WHERE `host` IS NULL;

소나 스키마 버전을 235로 변경 - 로그프레소 셸에서 다음 명령어 수행

> sonar.setSchemaVersion 235

로그프레소 셸에서 나머지 마이그레이션 수행 - 로그프레소 셸에서 다음 명령어 수행

> sonar.migrate

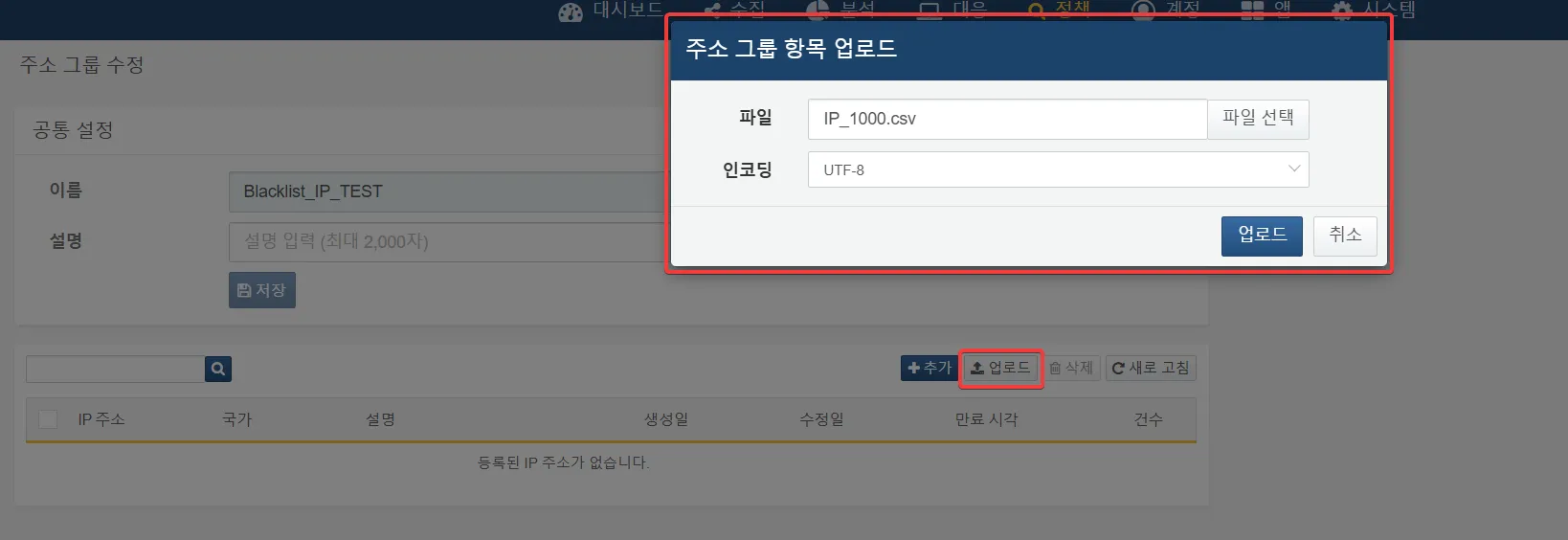
#### SNR#2589 위협 인텔리전스 조회, 활성화, 비활성화 REST API 추가

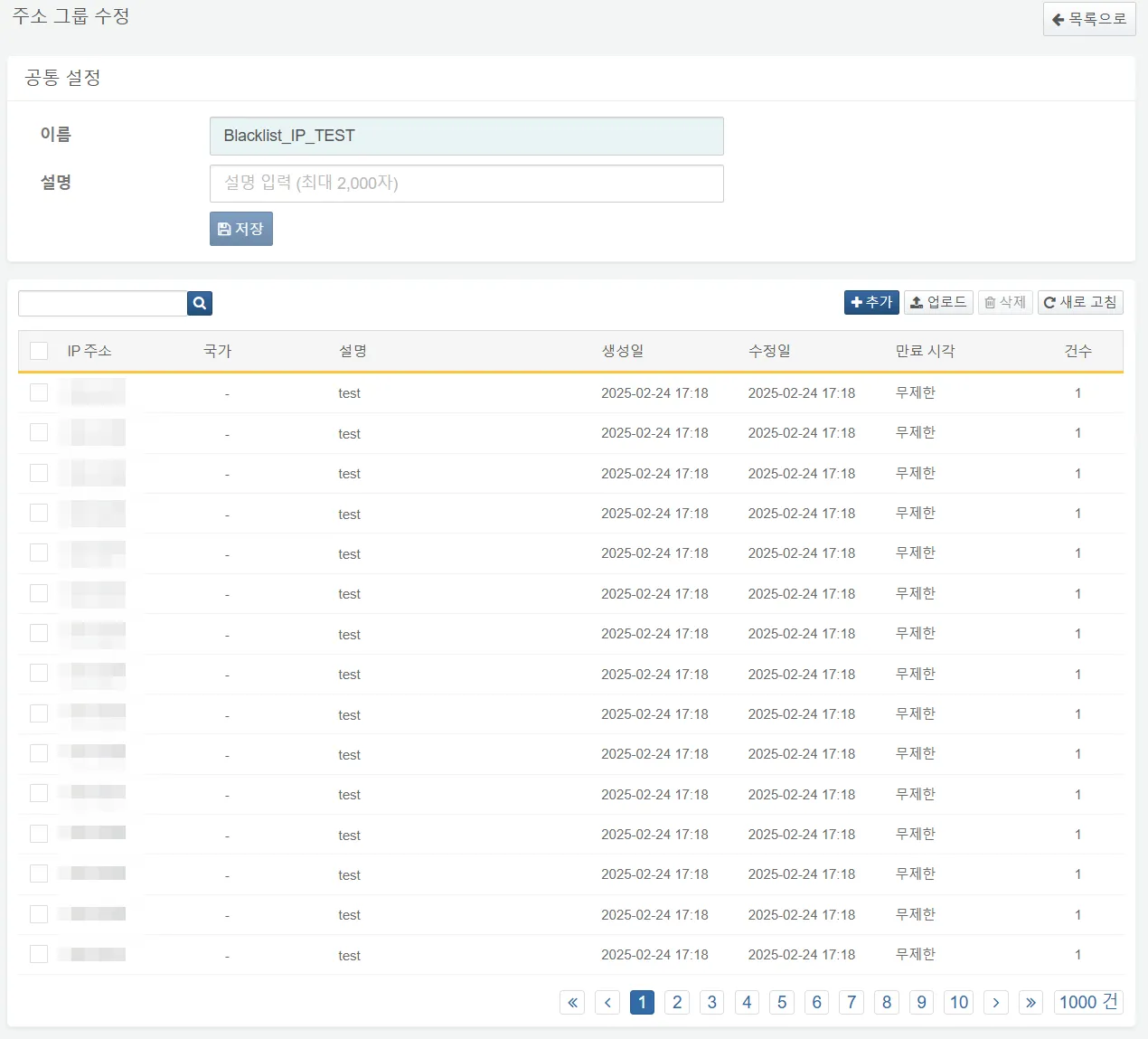
위협 인텔리전스 REST API가 추가되었습니다.

* [위협 인텔리전스 피드 목록 조회](https://docs.logpresso.comnull)
* [위협 인텔리전스 피드 활성화](https://docs.logpresso.comnull)
* [위협 인텔리전스 피드 비활성화](https://docs.logpresso.comnull)

#### SNR#2631 주소 그룹 대용량 업로드 기능 추가

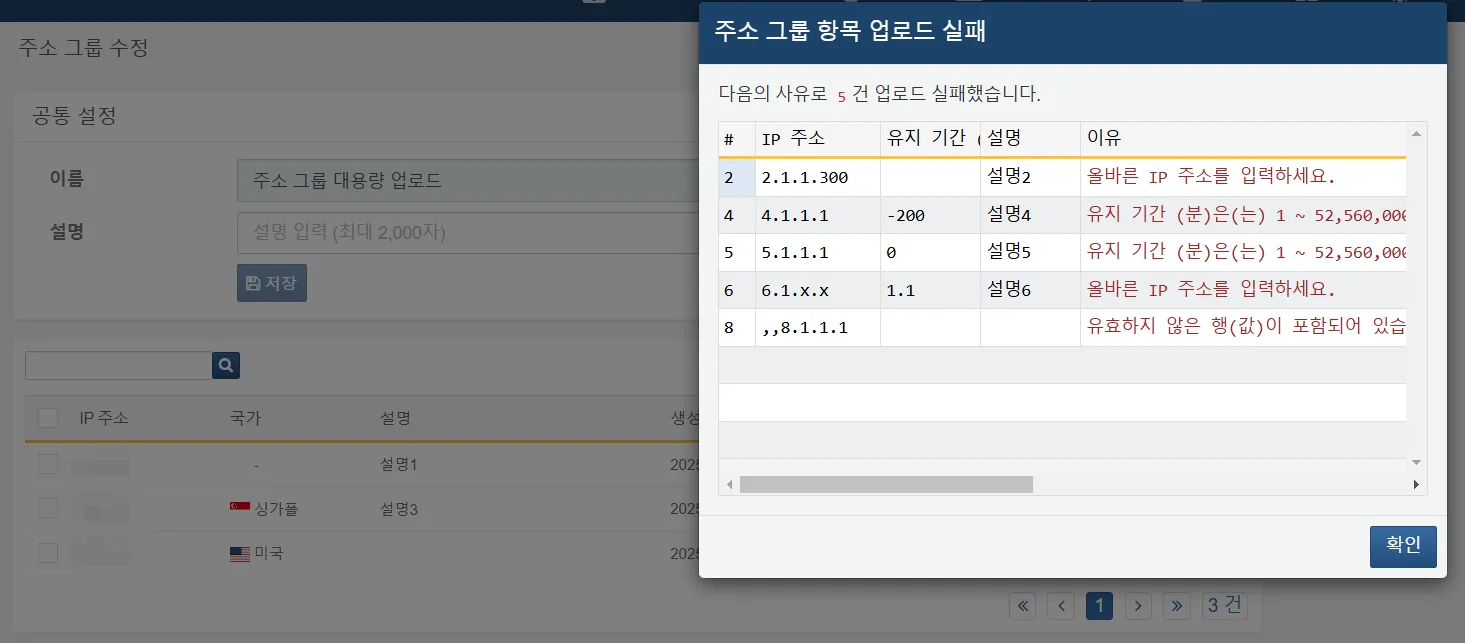
CSV 파일을 업로드하여 주소 그룹에 IP 주소를 대용량으로 추가하는 기능이 추가되었습니다. 한 번에 업로드할 수 있는 IP 주소 개수는 10,000건입니다. 하나의 주소 그룹에 들어갈 수 있는 IP 갯수는 1,000,000건 입니다.



업로드가 완료되면 완료 메시지가 표시되고 다음과 같이 IP 주소가 추가됩니다.

CSV 파일은 다음 필드를 가져야 합니다.

* address : IP 주소
* description : 설명
* period : 유지 기간 (분)

업로드하는 CSV 파일에 잘못된 행이 있는 경우, 정상적인 행에 대해서만 부분 성공합니다. (8건 중 3건만 성공)

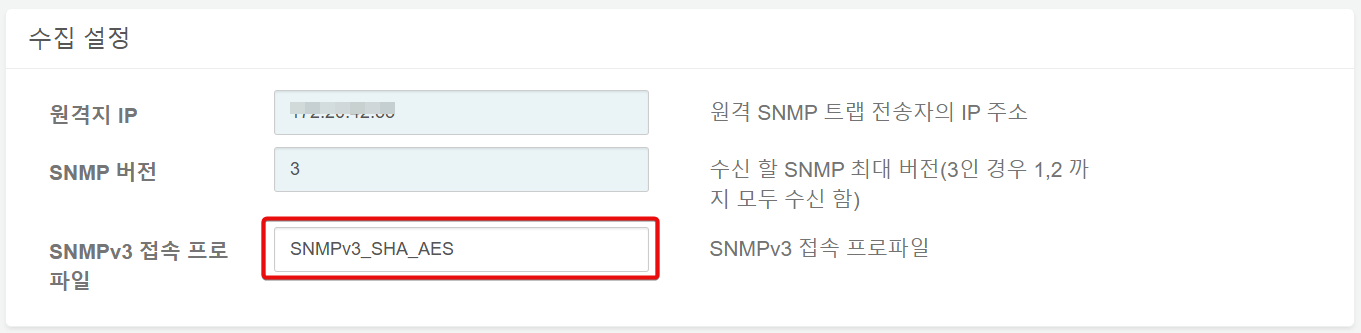
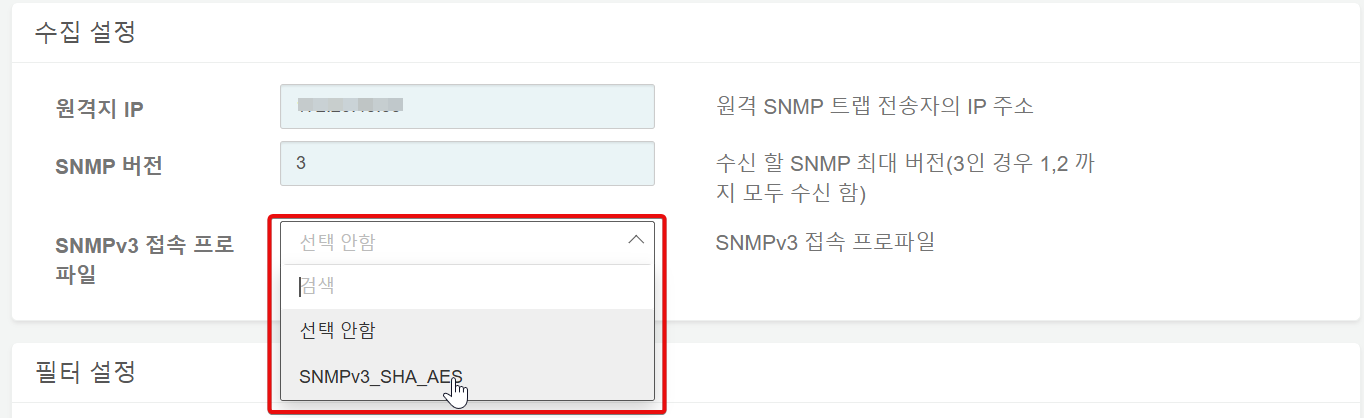
#### SNR#2846 로그프레소 런처 배포

로그프레소를 설치, systemd 등록, 구동, 중지할 수 있는 런처 기능이 공식 배포되었습니다. 기존에 사용하던 run.sh, config.sh 를 대체합니다. 구체적인 사용법은 다음과 같습니다.

* 사전 준비
* 로그프레소 설치 명령을 수행하기 위해선 root 권한이 필요합니다. 권한이 없을 경우 오류 메시지를 표시합니다.
* $ ./logpresso install server error: install requires root privileges.
* 런처를 사용하기 위해선 JAVA\_HOME 변수를 설정해야 합니다.
* $ export JAVA\_HOME=/opt/logpresso/jdk-11.0.14.1-jemalloc
* JAVA\_HOME 변수를 설정하지 않으면 오류 메시지를 표시합니다.
* $ sudo ./logpresso Error: JAVA\_HOME is not defined correctly. We cannot execute
* systemctl 기능을 사용하기 위해선 로그프레소 설치 경로에 jre 심볼릭 링크를 생성해야 합니다.
* $ ln -s jdk-11.0.14.1-jemalloc jre
* jre 심볼릭 링크가 없을 경우 아래와 같이 구동에 실패합니다.
* $ systemctl start logpresso Job for logpresso.service failed because the control process exited with error code. See "systemctl status logpresso.service" and "journalctl -xeu logpresso.service" for details.
* 설정 파일 생성
* 신규 설치를 하는 경우든 기존에 run.sh를 쓰다가 런처로 전환하는 경우든, 런처를 통해 로그프레소를 구동하기 위해서는 런처 설정 파일이 필요합니다. logpresso install config 명령을 수행하면 logpresso.conf 파일을 생성합니다.
* $ ./logpresso install config configuration file is created: /logpresso/etc/logpresso.conf $ vi ./etc/logpresso.conf
* 설정 파일에서 필요한 항목을 설정합니다. 예를 들어 로그프레소 셸 SSH 접근을 허용하려면 아래와 같이 logpresso.conf 파일을 수정합니다.
* # Parameter: -Daraqne.ssh.server # Default: disabled # Value: disabled | enabled SSH\_OPEN="enabled"
* 로그프레소 설치
* install server 명령어로 로그프레소 서버를 설치할 수 있습니다.
* $ ./logpresso install server
* 로그프레소 systemd 등록
* install systemd-service로 로그프레소를 systemd에 등록할 수 있습니다. systemd에 등록하면 systemctl을 통해 로그프레소를 시작하거나 중지할 수 있으며, 서버 부팅 시 자동으로 시작되도록 systemctl enable 설정을 할 수 있습니다.
* $ ./logpresso install systemd-service
* 로그프레소 구동 및 중지
* start 명령어로 로그프레소를 구동합니다.
* $ ./logpresso start
* stop 명령어로 로그프레소를 중지합니다.
* $ ./logpresso stop

#### SNR#2527 SNMP 트랩 수집기 설정에서 접속 프로파일 드롭다운 선택 기능 추가

SNMP 트랩 수신기에서 SNMP v3 트랩 데이터를 수신할 때, 이전에는 SNMPv3 접속 프로파일의 이름을 찾아서 직접 입력하는 번거로움이 있었습니다. 이제 등록된 SNMPv3 접속 프로파일 중 하나를 선택하여 지정할 수 있습니다.

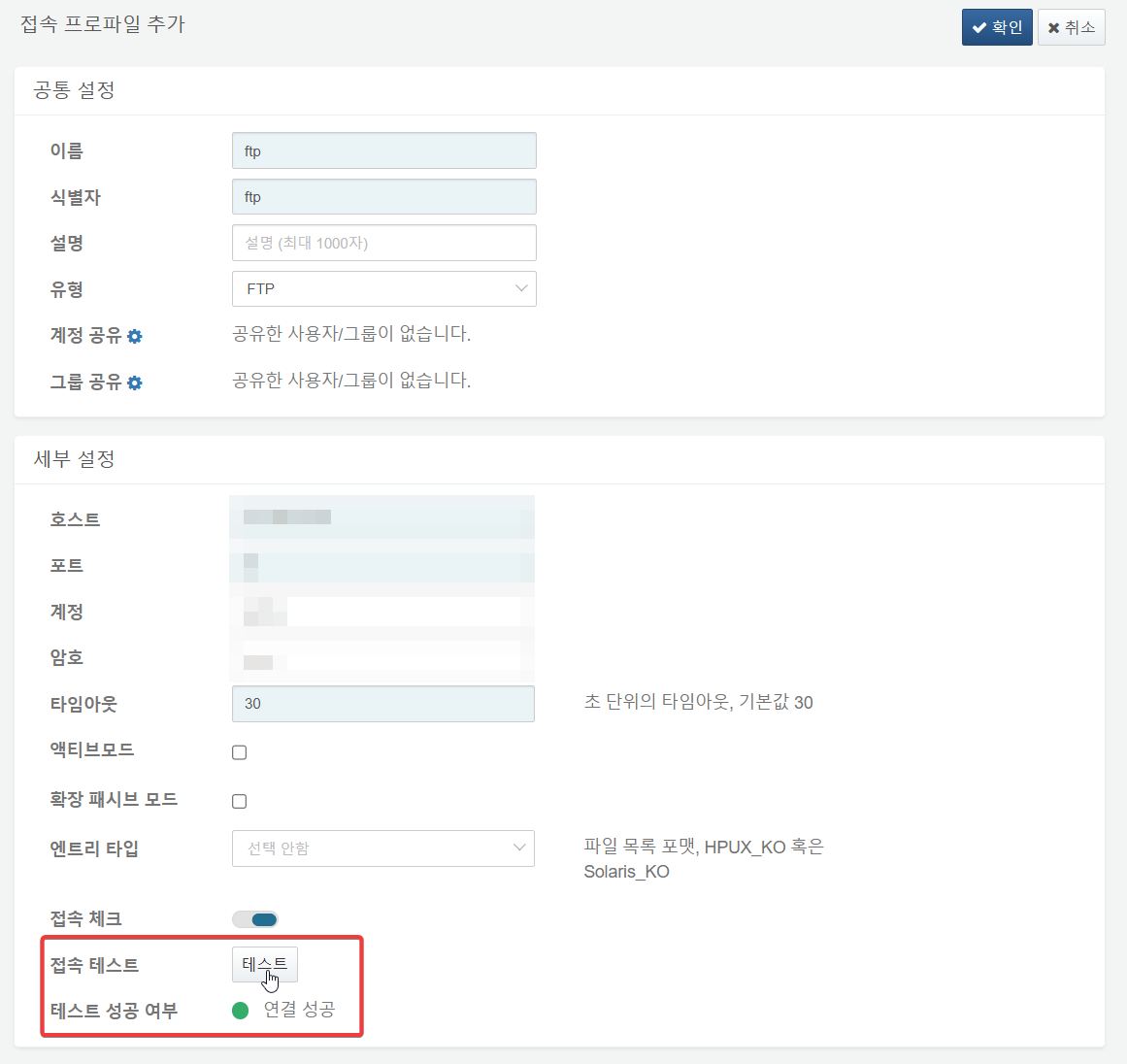
* 기존 SNMP 트랩 수신기의 SNMPv3 접속 프로파일 입력
* 
* 4.0.2502.0 버전 SNMP 트랩 수신기의 SNMPv3 접속 프로파일 선택
* 

#### SNR#2530 접속 프로파일의 접속 상태를 확인할 수 있는 기능 추가

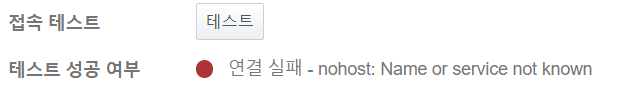
* 접속 프로파일의 접속 가능 상태를 확인해주는 기능을 추가했습니다.

접속 상태 확인은 내장 접속 프로파일 유형 중 FTP, SSH, 데이터베이스 유형에 대해서만 제공합니다. 그 외 로그프레소 CTI, LDAP, 앱에 포함된 접속 프로파일 등은 접속 체크 기능을 제공하지 않습니다.

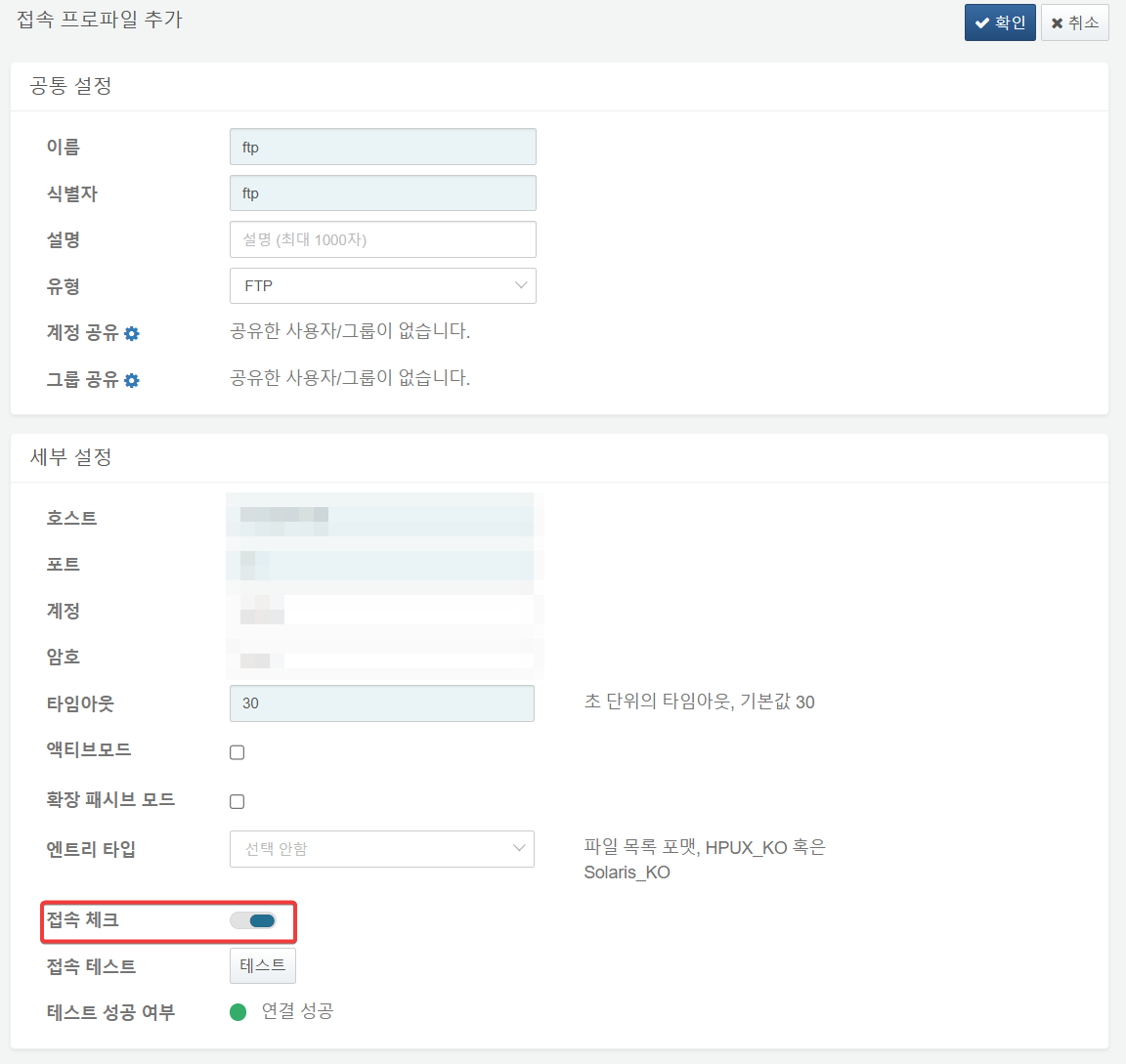
접속 프로파일 설정 화면에서 "접속 테스트" 버튼을 클릭해서 현재 입력한 정보로 접속 테스트를 진행할 수 있습니다.



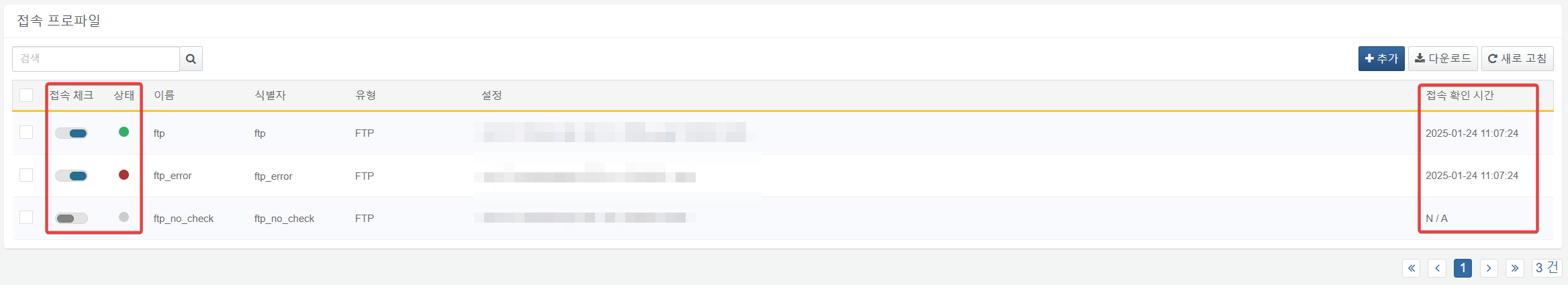
입력한 정보가 잘못된 경우, 연결에 실패하고 실패 사유가 표시됩니다.



접속 프로파일의 "접속 체크" 기능을 활성화하면 접속 프로파일의 연결 상태를 수시로 체크할 수 있습니다.



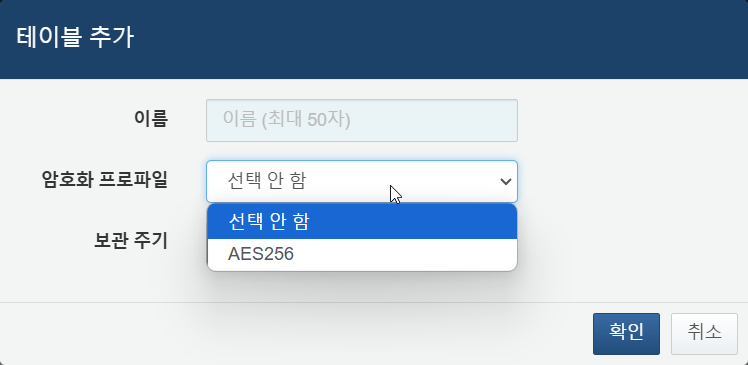
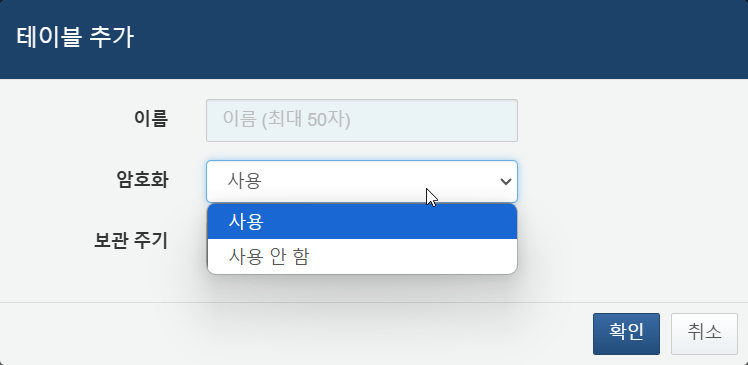
접속 체크 상태에 따라 접속 프로파일 목록에서 상태를 성공(초록)이나 실패(빨강)를 표시하고, 접속 체크를 비활성화한 접속 프로파일은 회색으로 표시됩니다.



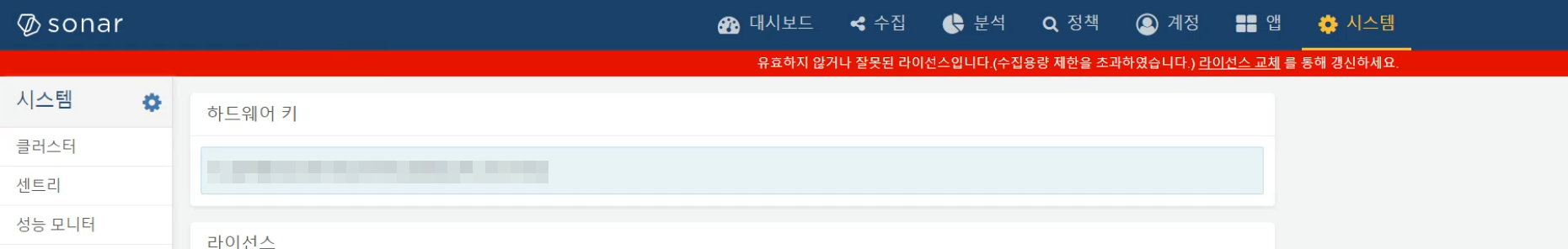
#### SNR#2538 스토리지 인증서 동기화 기능 추가 및 테이블 암호화 설정 방법 변경

* 테이블 암호화 프로파일용 스토리지 인증서가 다른 노드에 동기화되지 않는 현상이 해결되었습니다.

4.0.2502.0 이전 버전에서 패치를 진행하는 경우에는 패치 전 반드시 다른 노드에 스토리지 인증서를 동기화해야 합니다.

* 암호화 프로파일 메뉴가 사라지고, 테이블 암호화 시, 암호화 프로파일을 선택하는 것이 아닌 암호화 여부를 묻는 방식으로 변경되었습니다.
* 패치 전: 암호화 프로파일을 선택해야 함
* 
* 패치 후: 암호화 사용 여부를 선택함
* 

#### SNR#2547 라이선스 경고 표시 기능 추가

* 라이선스 메뉴 관련 아래의 항목들이 개선되었습니다.
* 라이선스 화면에서 모든 하드웨어 키를 표시하도록 개선
* 하드웨어 키 목록에서 모든 하드웨어 키를 표시하도록 변경했습니다.
* 라이선스 발급 시 입력한 모든 하드웨어 키를 표시하도록 변경했습니다.
* 
* 라이선스가 유효하지 않은 경우, 웹콘솔 화면 상단에 라이선스 경고 메시지를 표시하고 라이선스 목록에서 라이선스 경고 유형에 따른 색상을 표시합니다.
* 상단 경고 메시지
* 
* 기술 지원 기간을 초과한 라이선스 (노랑)
* 유효 기간을 초과한 라이선스 (주황)
* 비정상적인 라이선스 (빨강)
* 
* 라이선스 아이콘을 변경했습니다.
* (변경) STD → LIGHT
* (변경) ENT → LIGHT-HA
* (유지) SONAR
* (유지) MAE

#### SNR#2565 수집기 목록 조회 성능 개선

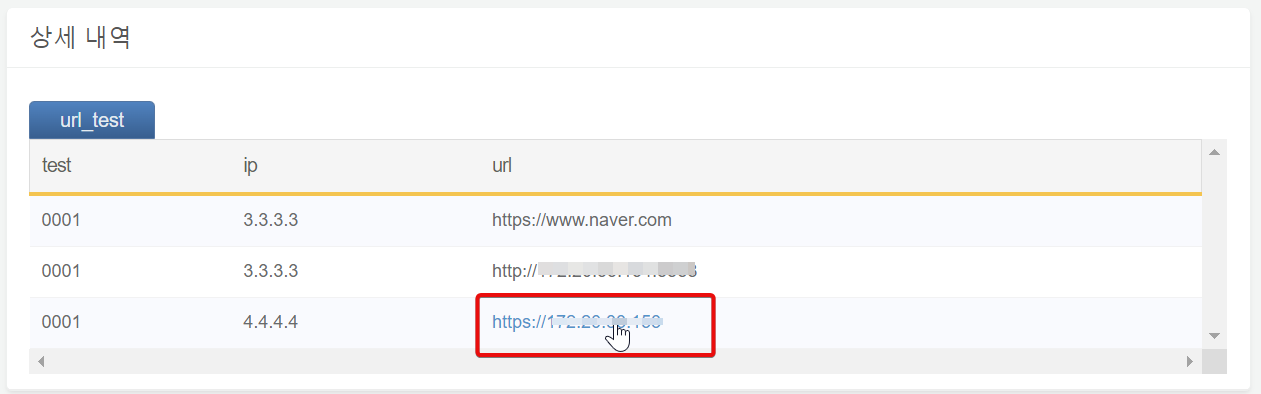
대량 클러스터 환경에서 노드가 수십 대 이상 존재하거나 센트리가 수백 대 이상 존재할 때 수집기 목록 조회 동작이 수 초 이상 걸리는 문제가 해결되었습니다. 수집기 통계 정보를 비동기적으로 조회하도록 수정하여 목록 조회 성능을 개선했으며, 다만 이로 인해 수집기 목록 조회 시 수집 건수 및 용량 반영이 지연될 수 있습니다.

#### SNR#2599 쿼리 REST API 출력 type에 단일 JSON 파일 유형 추가

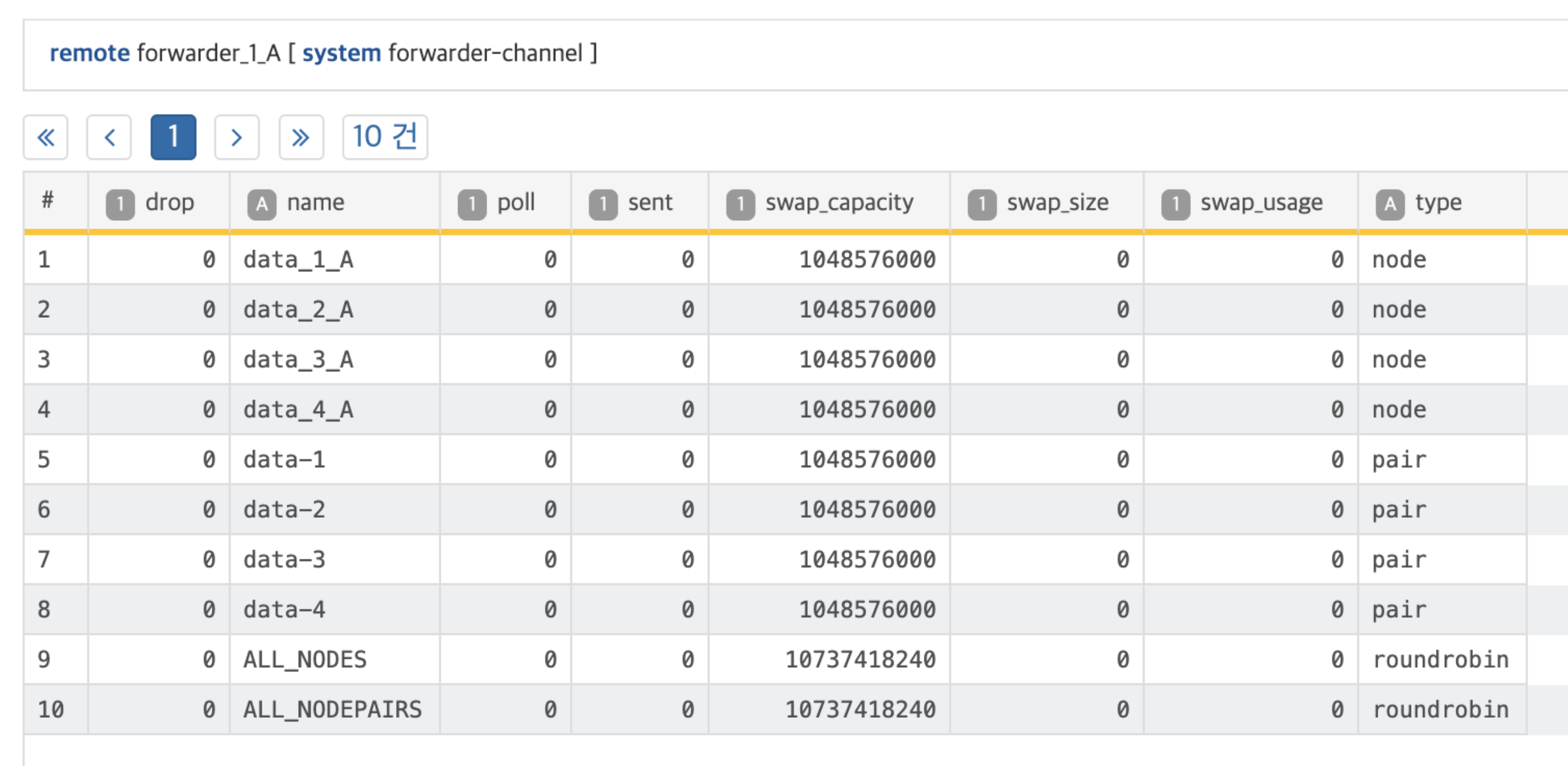
쿼리 REST API의 TYPE 매개변수 값으로 기존 html, txt, xml, csv, json에 jsonlines 유형을 추가했습니다.

#### SNR#2604 소명 상세 근거 항목에 URL 필드가 존재하면 하이퍼링크로 변환하는 기능 추가

소명 상세 내역에서 http:// 혹은 https:// 로 시작되는 값이 있을 때, 클릭 가능한 링크로 전환하는 기능을 추가했였습니다. 링크 클릭 시 새 탭에서 해당 주소가 열립니다.



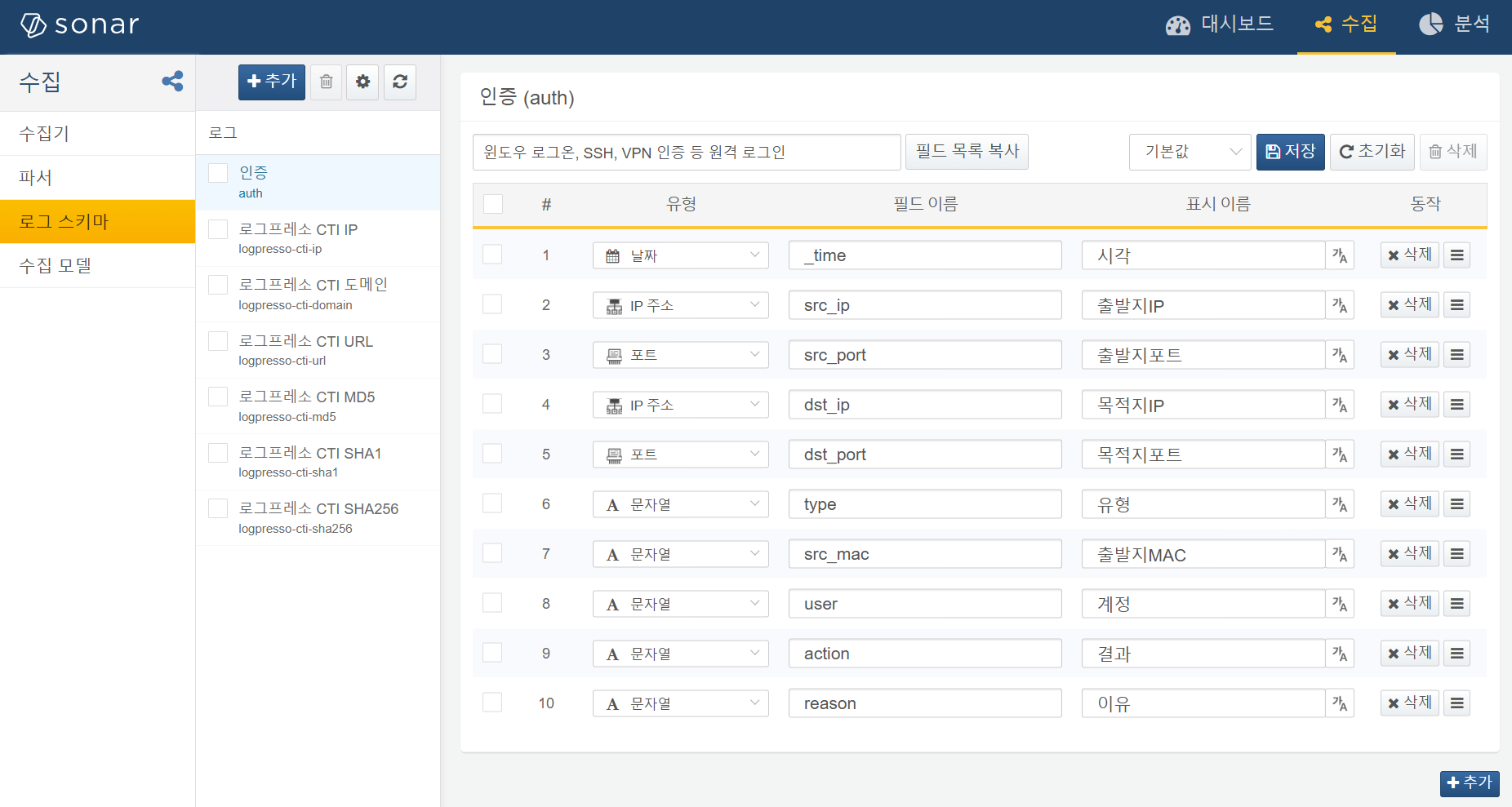
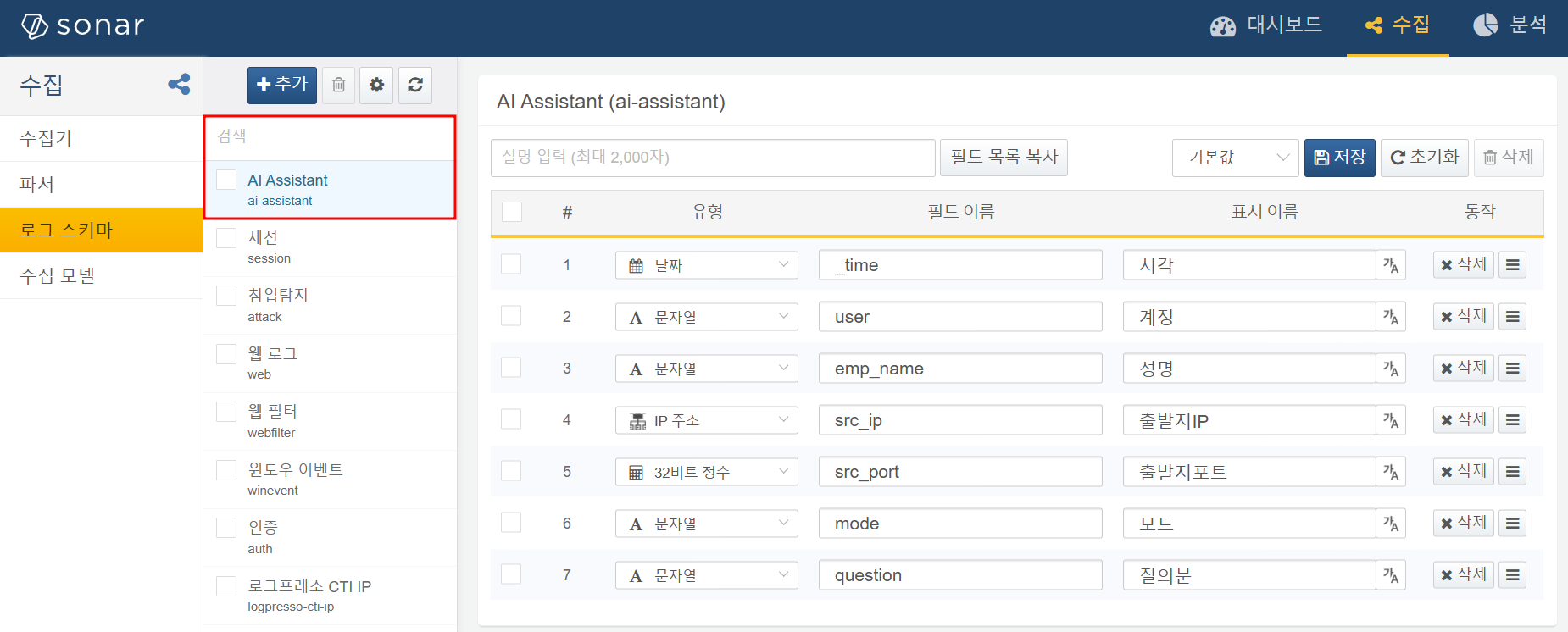
#### SNR#2621 전달 서버 데이터 전송 로직 개선 및 스왑 용량 확인 쿼리 명령어 추가

* 전달 서버에서 수집 서버로 로그를 전달 시 대기시간을 단축했습니다.
* 전달 서버의 스왑 용량 확인 및 변경 기능이 추가 되었습니다. 쿼리 명령어는 분석 서버가 아닌 전달 서버에서 수행해야 합니다. remote 쿼리 명령어를 사욯해서 수행할 수 있습니다.
* 스왑 용량 확인 쿼리 명령어 : system forwarder-channel
* 
* 전달 서버에 연결된 노드의 스왑량이 표시 됩니다.
* 스왑 용량 변경을 위해선 수집 서버에서 다음 로그프레소 셸 명령어를 수행합니다. forwarder.setSwap [채널명] [사이즈]
* logpresso> forwarder.setSwap ALL\_NODEPAIRS 83886080000 swap capacity changed
* 스왑 용량 변경 시 기 설정된 스왑 사이즈보다 작으면 변경이 실패 합니다.
* logpresso> forwarder.setSwap ALL\_NODEPAIRS 83886080 error: cannot shrink swap

스왑의 목적은 수집 지연으로 인한 로그 유실을 방지하는 것으로 용량이 부족할 시엔 스왑 용량을 늘려 유실을 방지할 수 있습니다. 다만 이 때 디스크 용량을 더 많이 사용할 수 있습니다.

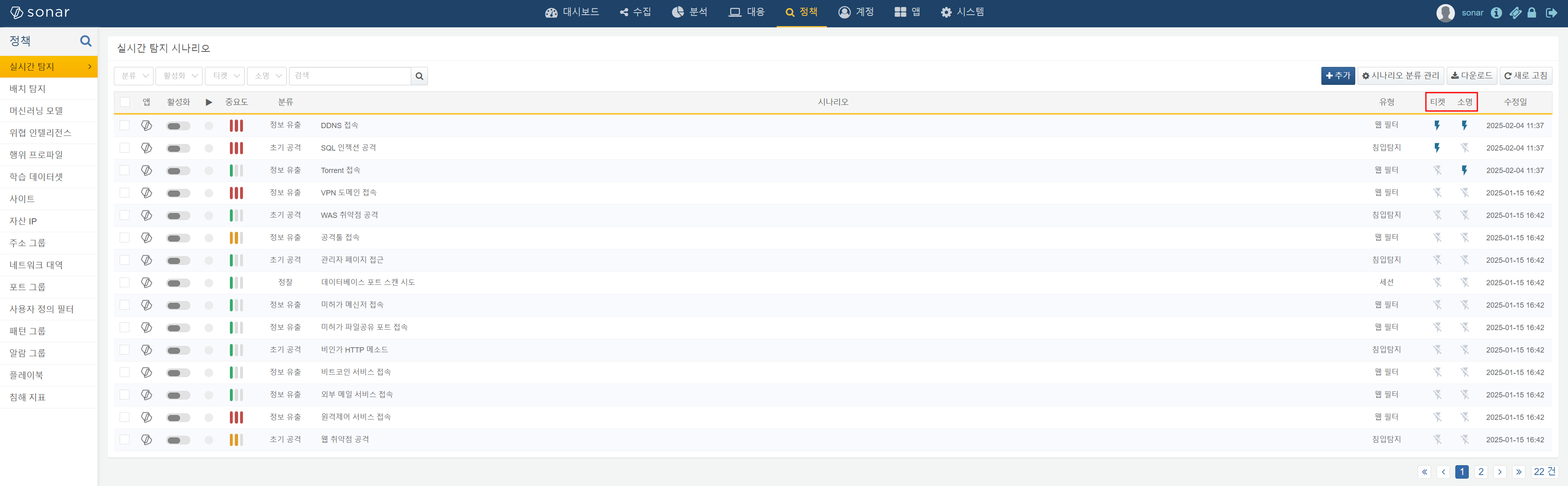
#### SNR#2657 로그 스키마 검색 기능 추가

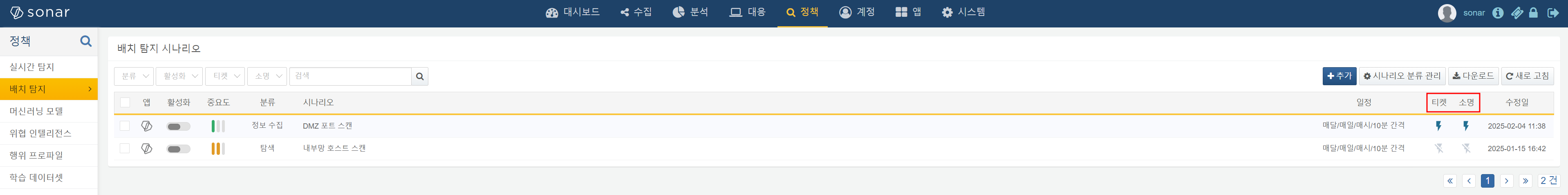
로그 스키마 검색 기능이 추가되었습니다. 로그 스키마 목록 위에 추가된 검색 창에 로그 스키마의 이름, 식별자, 설명을 검색할 수 있습니다. 영문의 경우 대소문자 구분 없이 검색합니다.



#### SNR#2658 시나리오 목록 화면에 소명/티켓 사용 여부 표시 칼럼 추가

탐지 시나리오 목록에서 소명이나 티켓이 발생하는지 여부를 표시하는 컬럼을 추가했습니다.





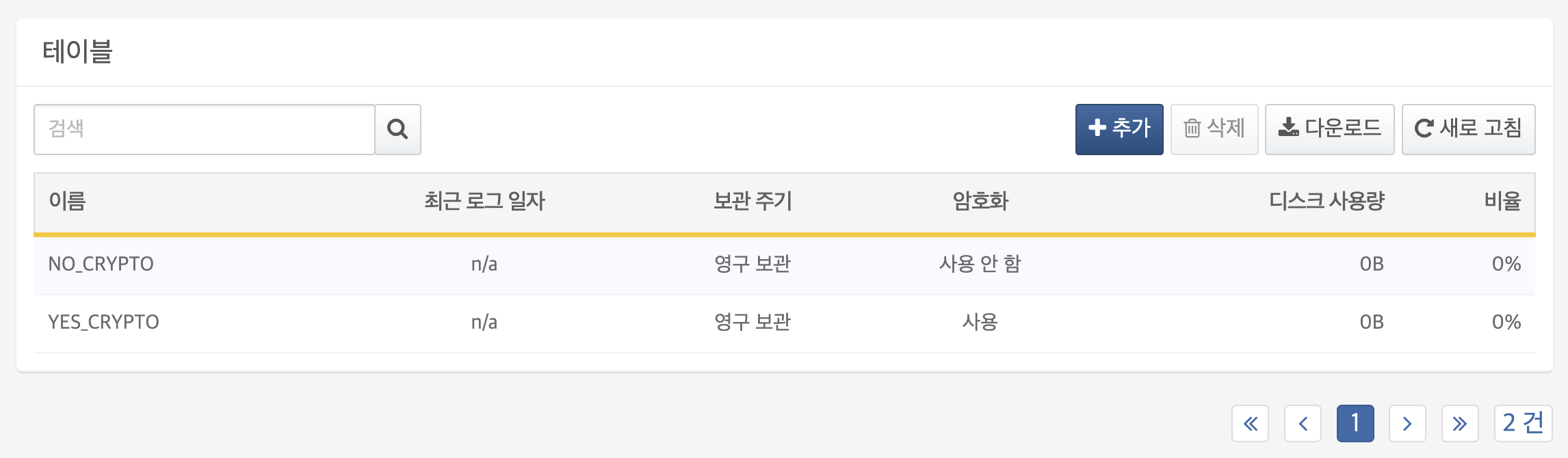
#### SNR#2666 센트리 자동 설치 시 사용자가 지정한 스크립트 사용 지원

소나 서버 설치 경로의 download/installer/ 하위 경로에 사용자 정의 설치 스크립트(install.sh 혹은 install.cmd)를 넣어두면 센트리 자동 설치 시 내장 스크립트 대신 사용자 정의 설치 스크립트를 사용할 수 있도록 수정했습니다.

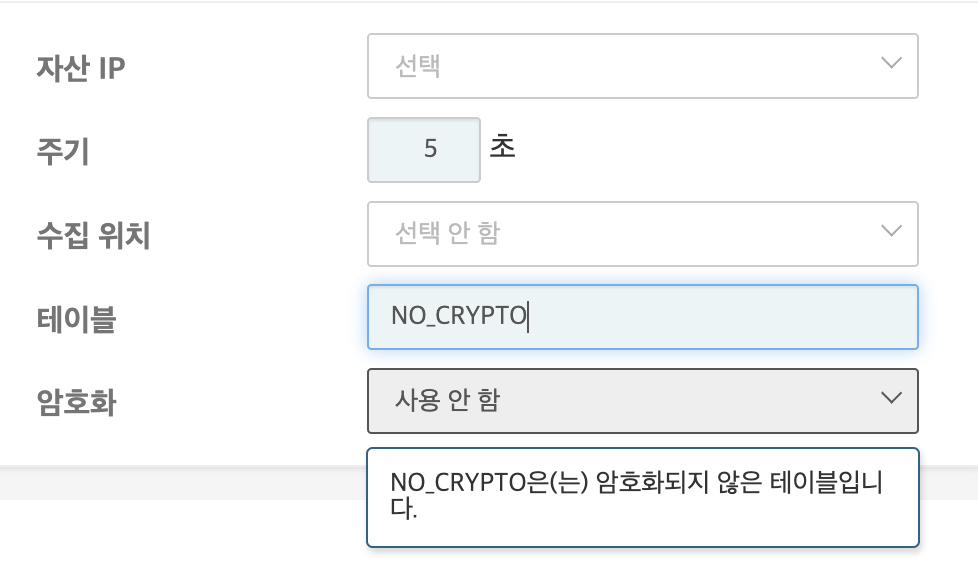
#### SNR#2674 수집기 생성 시 암호화한 테이블을 생성하는 기능 추가 및 기존 테이블 암호화 여부 표시 기능 추가

수집기 생성 시 입력한 테이블이 이미 존재하는 테이블이면 암호화 여부를 표시하고, 새로 생성할 테이블이면 암호화 여부를 선택할 수 있는 기능을 추가했습니다.

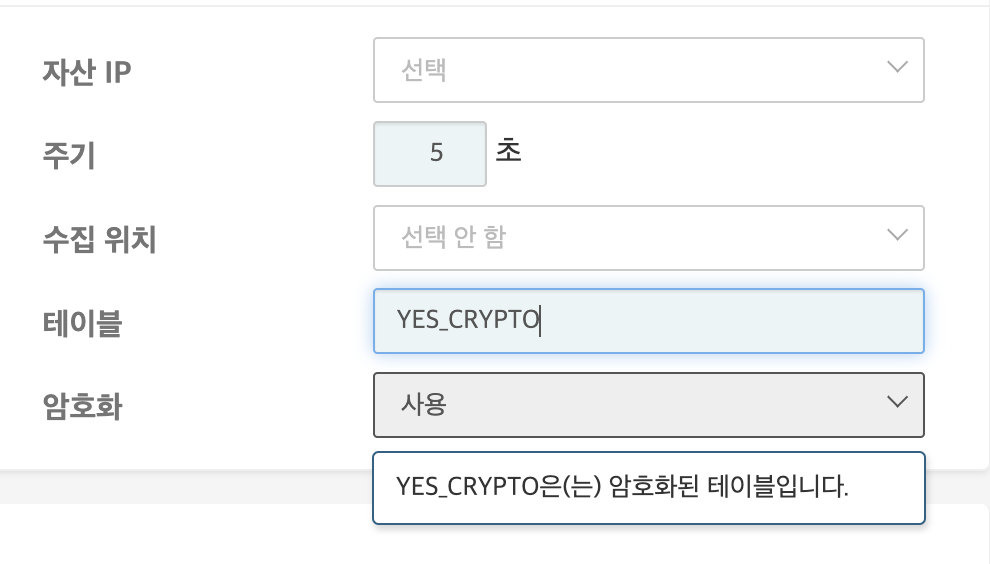
예시) 다음과 같이 암호화가 적용된 YES\_CRYPTO 테이블과 적용되지 않은 NO\_CRYPTO 테이블이 있다고 가정합니다.



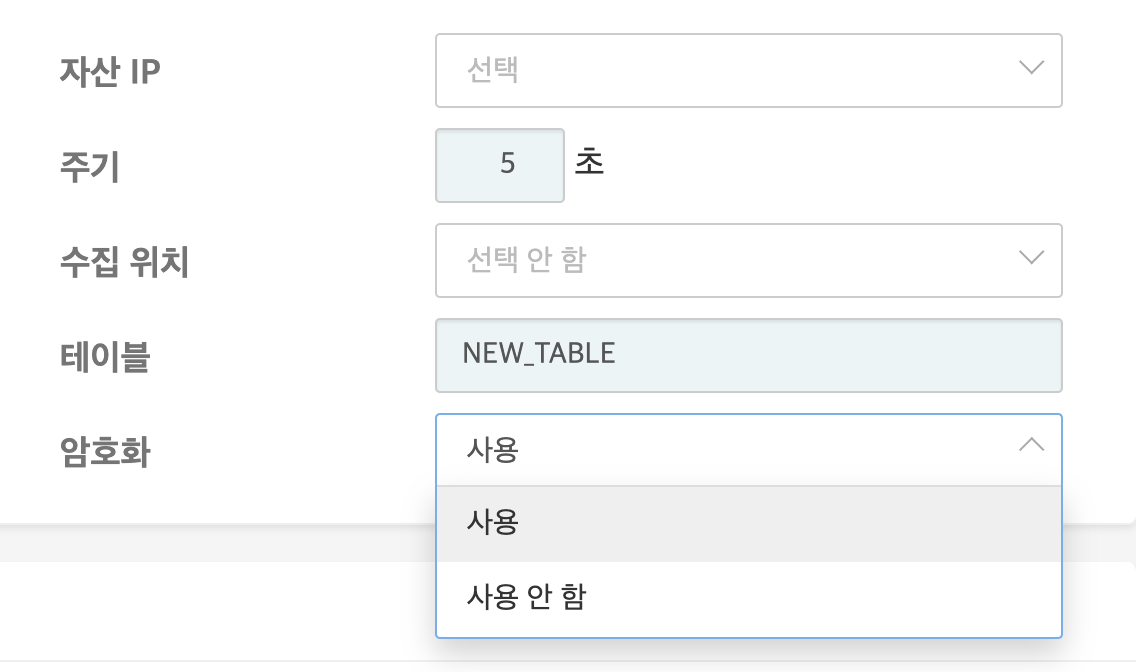
수집기 생성 시 테이블에 NO\_CRYPTO를 입력하면 암호화 항목은 "사용 안 함"으로 표시되고 변경할 수 없습니다.



수집기 생성 시 테이블에 YES\_CRYPTO를 입력하면 암호화 항목은 "사용"으로 표시되고 변경할 수 없습니다.



수집기 생성 시 테이블에 신규 테이블인 NEW\_TABLE을 입력하면 테이블의 암호화 여부을 선택할 수 있습니다.



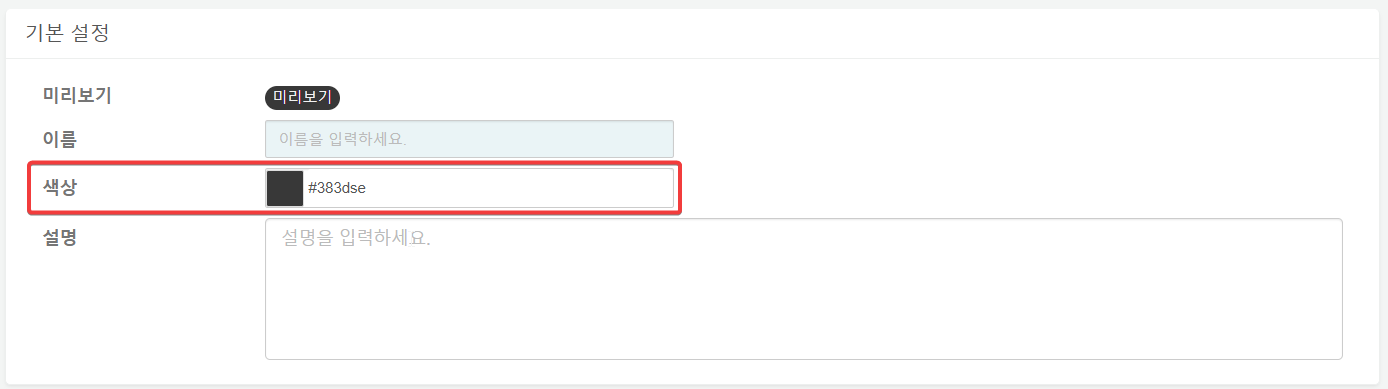
#### SNR#2722 ISAC 위협 인텔리전스 피드 제거

기존에 위협 인텔리전스 목록에서 제공하던 ISAC 항목들이 오랜 기간동안 정보가 갱신되지 않아 해당 항목들을 위협 인텔리전스 목록에서 제거했습니다.

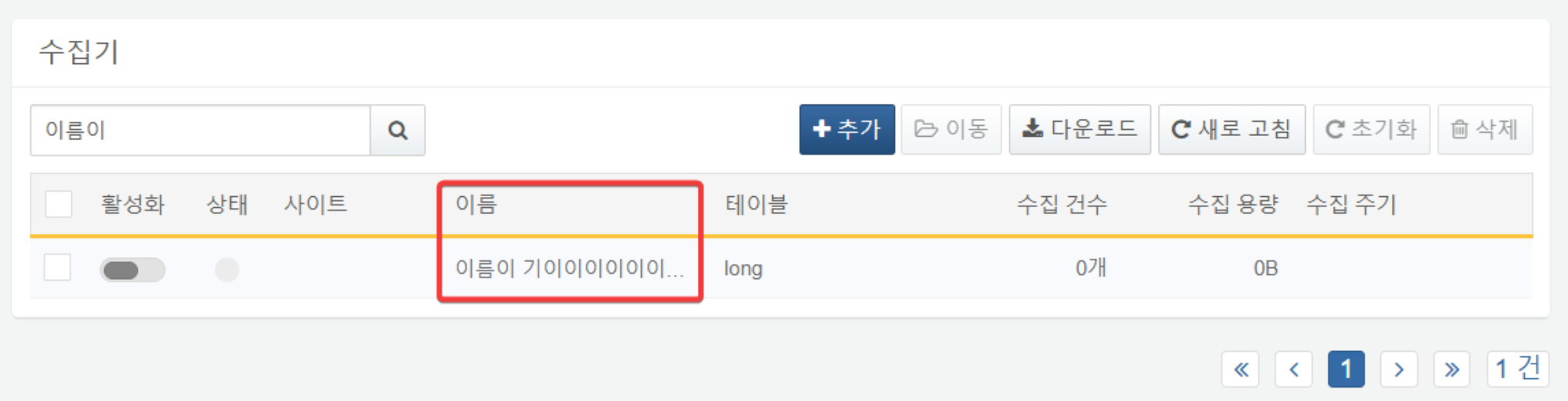
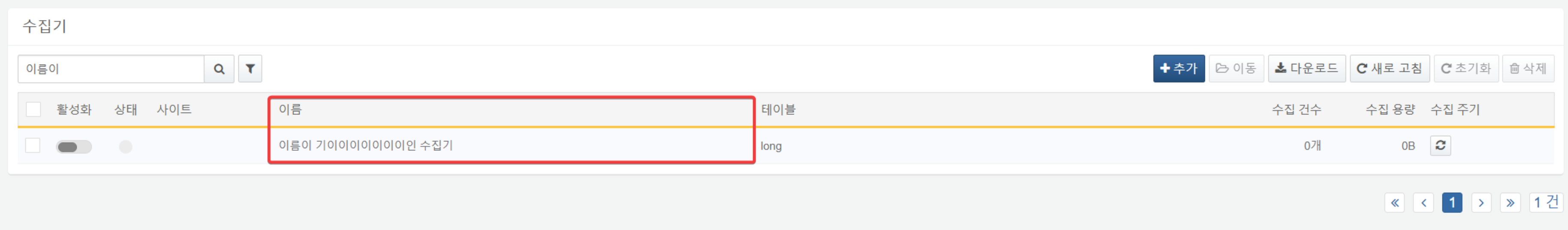
* 대상 위협 인텔리전스: otx, tor, mdl\_domain, mdl\_ip, abusech, malc0de

#### SNR#2740 티켓 태그 색상 입력 방식 개선

티켓 태그 생성/수정 시, 색상 입력란에 헥사코드를 직접 입력하여 색상을 지정할 수 있게 개선되었습니다.



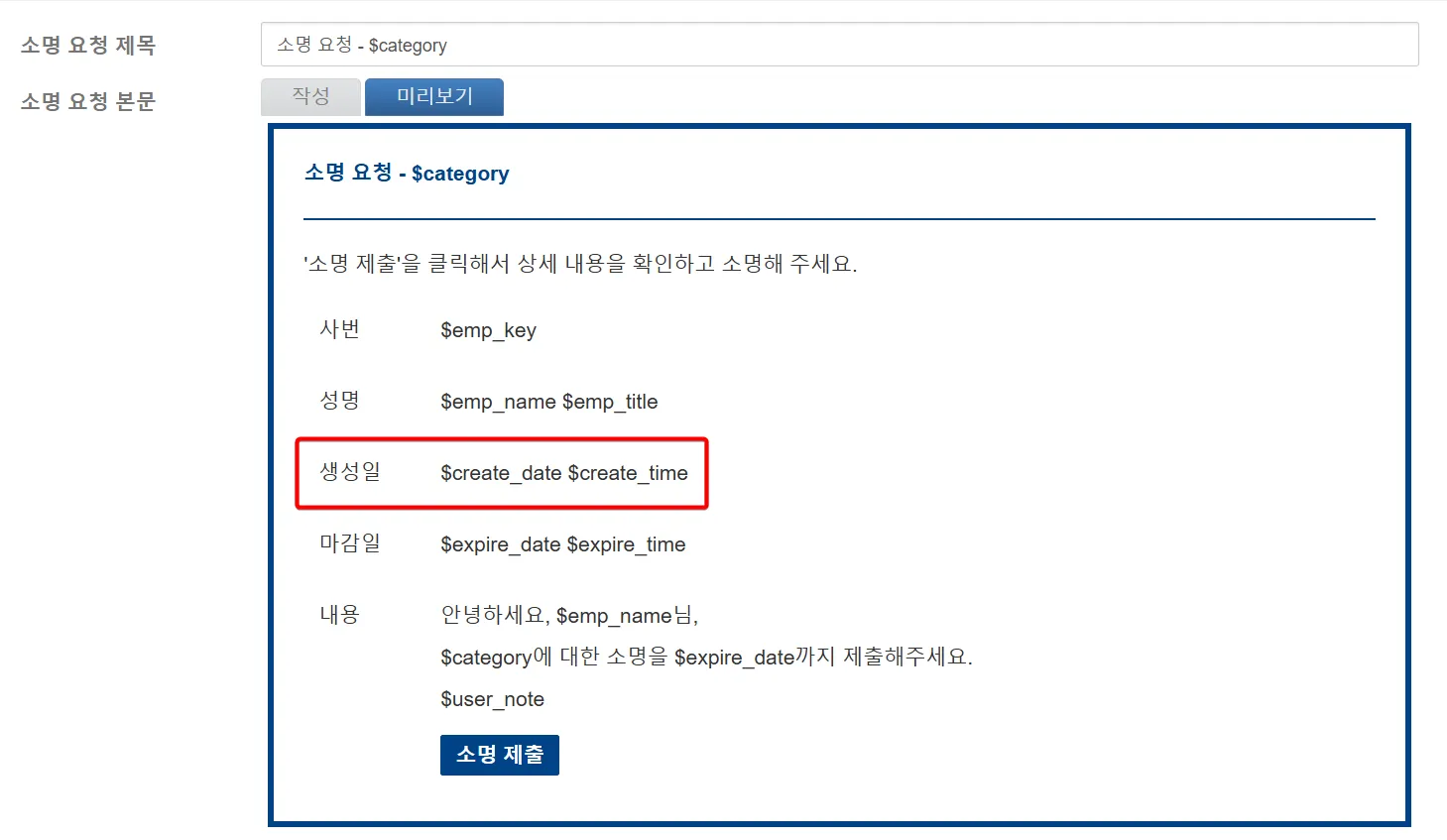
#### SNR#2741 수집기 화면 너비 확대

* 수집기 목록 너비가 넓어졌습니다.
* 패치 전 : 너비가 좁아 이름이 길면 축약 표시
* 
* 패치 후 : 너비가 넓어져 긴 이름도 표시 가능
* 

#### SNR#2753 배치 시나리오 실행 시 테이블 적재가 지연될 때 티켓 근거자료가 보이지 않는 문제 해결

배치 시나리오 실행 시 쿼리 완료 후 테이블 적재가 full gc 등으로 지연되는 상황이 발생할 때 티켓 근거 자료 화면에서 근거 자료가 보이지 않는 문제가 개선되었습니다. 이 문제는 티켓 기능과 배치 시나리오가 구현되었을 때부터 존재했습니다.

#### SNR#2756 소명 템플릿 매크로에 소명 생성일 추가

* 소명 요청 템플릿에 소명 요청일, 소명 요청 시각 매크로가 추가되었습니다.
* 소명 요청일 : $create\_date
* 소명 요청 시각 : $create\_time
* 소명 요청 매크로 입력
* 
* 소명 메일
* 

#### SNR#2764 SNMP 트랩 로그 개선

SNMP 트랩 메시지 수신 실패 시 araqne.log 에 관련 오류 로그가 남도록 개선되었습니다.

* 인증 프로토콜이 맞지 않는 경우

[2024-12-23 15:46:45.174] WARN (SnmpTrapServiceImpl) - logpresso snmp: auth failure event: address [x.x.x.x/41560], error [Authentication failure]

* 암호화 프로토콜이 맞지 않는 경우

[2024-12-23 15:47:37.005] WARN (snmp4j) - snmp4j snmp4j-MPv3 ASN.1 parse error: Data length > 4 bytes are not supported![2024-12-23 15:47:36.229] WARN (snmp4j) - snmp4j snmp4j-MPv3 ASN.1 parse error: Wrong ASN.1 type. Not a string: 75 at position 3

* 커뮤니티 값이 맞지 않는 경우

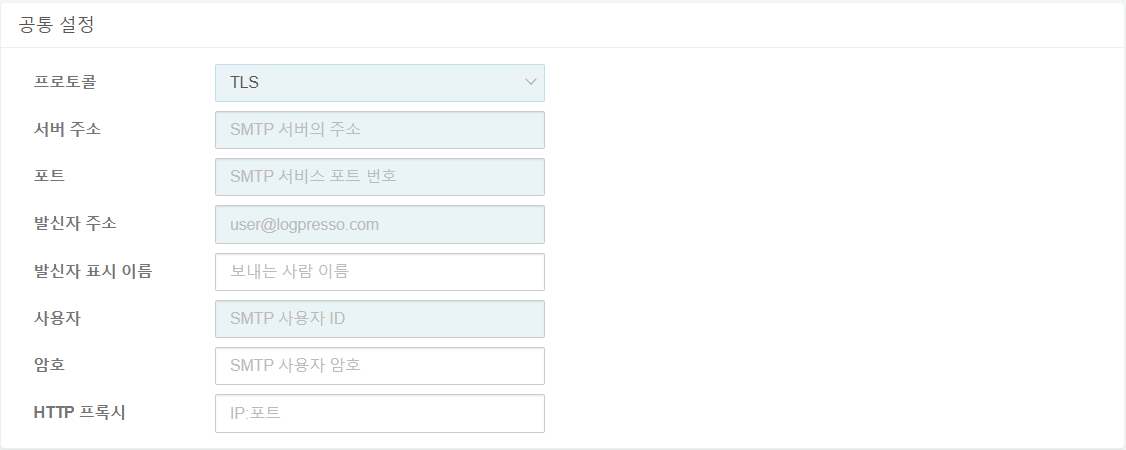
[2024-12-23 15:48:09.195] WARN (SnmpTrapServiceImpl) - logpresso snmp: auth failure event: address [x.x.x.x/43953], error [Unknown security name]

#### SNR#2765 생명주기 프로파일 생성 및 수정 시 직접 복사 옵션 추가

생명주기(Warm 및 Cold) 등록 및 수정 시, 직접 복사 여부를 선택할 수 있습니다. 직접 복사를 선택하면 기존 파일을 유지한 채, 대상 위치로 데이터를 새롭게 복사합니다. 직접 복사는 파일 이름 변경과 이동이 제한적인 WORM 스토리지와 같은 환경에서 선택해야 합니다.

#### SNR#2773 소나 메일 설정에 프록시 설정 추가

소나 메일 서버 설정에 HTTP 프록시 항목이 추가되었습니다. 메일 서버와의 통신이 해당 프록시를 통하도록 설정할 수 있습니다.



#### SNR#2792 예약된 쿼리 쿼리문 10,000자까지 지원

기존에는 예약된 쿼리 쿼리문을 2,000까지만 입력할 수 있어서 긴 쿼리문을 입력하는 데 제약이 있었습니다. 이번 릴리스에서 쿼리문의 길이 제한을 10,000자까지 확대하여 긴 쿼리문도 입력이 가능하도록 개선하였습니다.



#### SNR#2812 계정 추가 시 임직원 연결 기능 삭제

계정 추가 및 계정 수정 시 임직원 연결 기능이 제거되었습니다.



#### SNR#2598 윈도우 이벤트 수집기가 이벤트 XML 파싱을 실패할 때 간헐적으로 중단되는 문제 해결

윈도우 이벤트 수집기가 간혹 수집한 이벤트 xml 의 파싱에 실패하는 경우 특별한 오류 메시지 없이 수집기가 중단되는 문제가 해결되었습니다.

#### SNR#2725 REST API IP 접근 제어 시 로드밸런서 구성 지원

로드밸런서 사용 시 REST API에 대한 계정 IP 접근 제어가 동작하지 않던 문제가 수정되었습니다. 이 문제는 REST API 지원이 시작된 4.0.2308.0 버전부터 발생되었습니다.

#### SNR#2727 sonar-set-ip-address 쿼리 명령어 사용 시 동일 IP가 추가되는 문제 해결

해당 이슈는 4.0.2308.0 버전부터 발생했습니다.

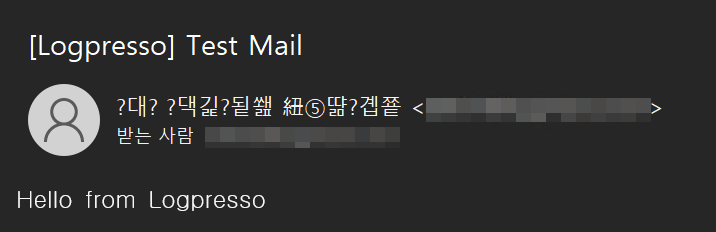
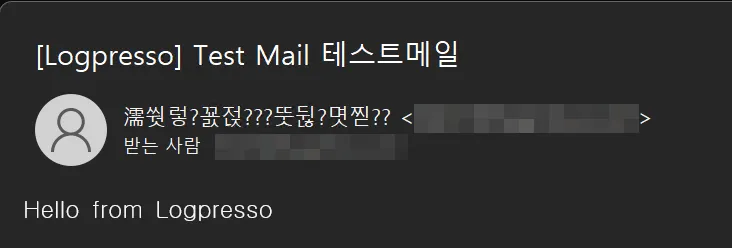
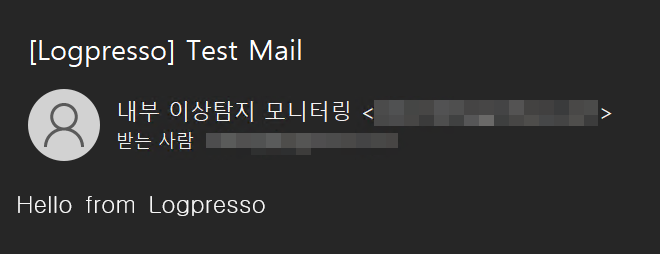
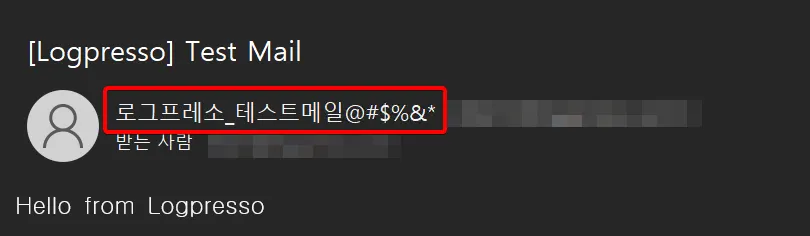
sonar-set-ip-address 쿼리 명령어에는 사이트 정보를 입력받는 옵션이 없는데 IP 저장 시에는 사이트와 IP를 함꼐 복합 유일키로 사용하고 있어서 유일키 비교가 정상적으로 이루어지지 않았습니다. 그래서 동일 IP를 입력하더라도 사이트 값이 null이어서 null 비교에서 false가 발생해서 동일 IP를 계속 입력할 수 있었습니다.

이를 해결하기 위해 [sonar-set-ip-address](https://docs.logpresso.comnull) 쿼리 명령어에 fields 옵션으로 사이트GUID를 입력할 수 있도록 수정했습니다.



#### SNR#2731 일부 메일 클라이언트에서 메일 발신자 이름이 정상적으로 표기되지 않는 문제 해결

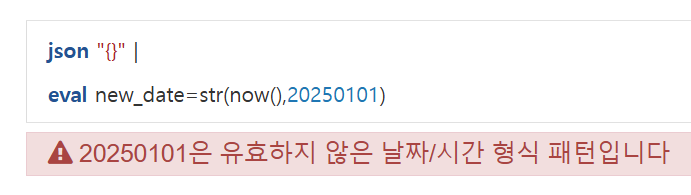
소나 메일 서버 설정의 발신자에 영문이나 숫자가 아닌 문자(non-ascii)가 포함되어 있을 때, 일부 메일 클라이언트에서 발신자가 정상적으로 표시되지 않는 문제가 수정되었습니다.

* 패치 전
* 패치 후

#### SNR#2745 string() 함수 사용시 날짜 지시자 형식이 잘못된 경우 NPE 오류 발생 해결

쿼리문에서 string() 혹은 str() 함수를 사용해 문자열을 날짜 형식으로 변환하려 할 때, 날짜 지시자 파라미터가 문자열 타입이 아닌 경우 NPE가 발생하던 문제를 해결했습니다. 패치 후 문자열 타입이 아닌 날짜 지시자를 입력하면 유효하지 않은 형식이라는 오류 메시지를 출력합니다.

[2024-12-01 00:28:59.968] ERROR (QueryTaskRunner) - araqne logdb: query [38611962] task [query: 38611962 scan: json "{}"] failedjava.lang.NullPointerException at java.base/java.text.SimpleDateFormat.<init>(SimpleDateFormat.java:617) at java.base/java.text.SimpleDateFormat.<init>(SimpleDateFormat.java:599) at org.araqne.logdb.query.expr.ToString.convert(ToString.java:157) at org.araqne.logdb.query.expr.ToString.eval(ToString.java:120) at org.araqne.logdb.query.command.Eval.update(Eval.java:97) at org.araqne.logdb.query.command.Eval.update(Eval.java:100) at org.araqne.logdb.query.command.Eval.onPush(Eval.java:127) at org.araqne.logdb.QueryCommandPipe.onRowBatch(QueryCommandPipe.java:39) at org.araqne.logdb.QueryCommand.pushPipe(QueryCommand.java:267) at org.araqne.logdb.query.command.Json.run(Json.java:46) at org.araqne.logdb.DriverQueryCommand$ScanTask.run(DriverQueryCommand.java:74) at org.araqne.logdb.query.engine.QueryTaskRunner.run(QueryTaskRunner.java:57) at org.araqne.logdb.impl.QueryThreadPoolServiceImpl$NamedRunnable.run(QueryThreadPoolServiceImpl.java:129) at java.base/java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1128) at java.base/java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:628) at java.base/java.lang.Thread.run(Thread.java:829)

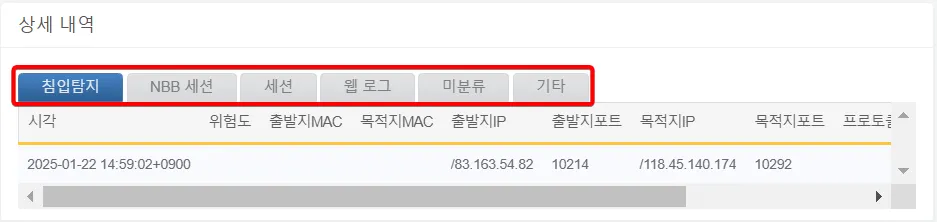


#### SNR#2748 null 값만 존재하는 필드에 대해 dc() 집계 함수 수행 시 결과가 0이 아닌 null이 나오던 문제 해결

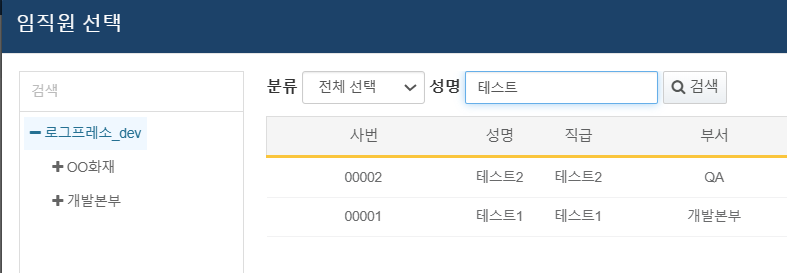
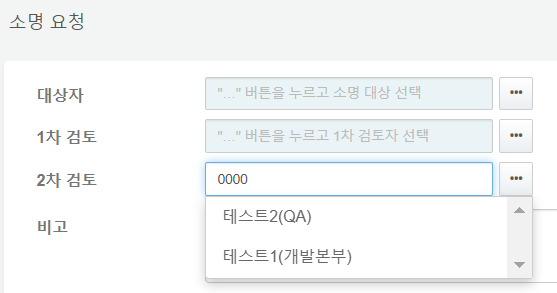
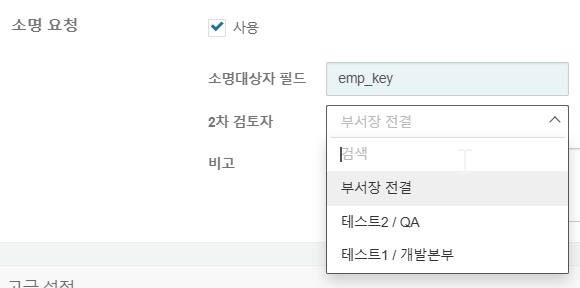
입력 데이터에서 해당 필드의 모든 값이 null인 경우 dc() 집계 함수를 사용해 통계 쿼리를 수행하는 경우 결과로 0이 아닌 null이 나오던 문제를 수정하였습니다.

#### SNR#2755 소명 근거자료 탭 정렬 시 미분류와 기타 탭이 제일 마지막 순서로 오도록 수정

소명 근거자료 탭 순서가 로그 스키마의 식별자를 기준으로 이름순 정렬이 되며, 로그 스키마가 없는 경우 순서 마지막에 미분류 > 기타 순서로 정렬됩니다.



#### SNR#2760 시나리오에서 소명 설정시 소나 계정이 없는 2차 검토자가 목록에 표시되는 문제 해결

* 소명 2차 검토자 검색 시, 소나 계정이 없는 임직원이 목록에 표시되는 현상이 해결되었습니다.
* 수동 소명
* 
* 자동 소명
* 

해당 이슈는 2019년도 패키지부터 발생했습니다.

#### SNR#2769 라이선스 연동 시 서버 타임존이 안맞는 경우 invalid-hash-code 오류 발생 해결

라이선스 마스터 노드와 슬레이브 노드간 타임존 설정 등이 맞지 않을 때 라이선스 동기화가 실패하며 다음 오류가 나는 문제가 수정되었습니다. 슬레이브 노드를 사용하는 모든 환경에서 발생할 수 있었습니다.

[2024-11-16 16:25:21.564] WARN (MessageBusImpl) - araqne msgbus: error message template [group\_id=logpresso, message\_id=invalid-hash-code, lang=en] not found[2024-11-16 16:25:21.564] ERROR (MessageBusImpl) - araqne msgbus: message handler failedorg.araqne.msgbus.MsgbusException: at com.logpresso.license.impl.LicenseServiceImpl.\_\_clgl(SourceFile:1470) at com.logpresso.license.impl.LicenseServiceImpl.clgl(SourceFile) at com.logpresso.license.impl.LicenseServiceImpl.\_\_onMasterNotify(SourceFile:1371) at com.logpresso.license.impl.LicenseServiceImpl.onMasterNotify(SourceFile)

#### SNR#2799 8192 바이트보다 큰 수집모델을 불러올 수 없는 문제 해결

크기가 8192 바이트를 넘는 수집 모델을 불러올 수 없는 문제를 해결했습니다. 마찬가지로 해당 수집모델을 포함한 앱도 설치할 수 없었던 문제를 해결했습니다. 앱 시스템이 추가된 4.0.2312.0 버전부터 발생한 문제입니다.

[2025-01-17 11:29:58,704] ERROR (AppResourceLoaderImpl) - sonar exchange: cannot load logger model [logger-model/secui-mf2.model] from bundle 146java.io.IOException: org.json.JSONException: A JSONObject text must begin with '{' at character 1 at com.logpresso.sonar.api.exchange.impl.LoggerModelExchangeServiceImpl.\_\_M\_loadJson(LoggerModelExchangeServiceImpl.java:305) at com.logpresso.sonar.api.exchange.impl.LoggerModelExchangeServiceImpl.loadJson(LoggerModelExchangeServiceImpl.java) at com.logpresso.sonar.api.exchange.impl.LoggerModelExchangeServiceImpl.\_\_M\_importAppLoggerModel(LoggerModelExchangeServiceImpl.java:413) at com.logpresso.sonar.api.exchange.impl.LoggerModelExchangeServiceImpl.importAppLoggerModel(LoggerModelExchangeServiceImpl.java) at com.logpresso.sonar.api.exchange.impl.AppResourceLoaderImpl.\_\_M\_importLoggerModels(AppResourceLoaderImpl.java:838) at com.logpresso.sonar.api.exchange.impl.AppResourceLoaderImpl.importLoggerModels(AppResourceLoaderImpl.java) at com.logpresso.sonar.api.exchange.impl.AppResourceLoaderImpl.\_\_M\_importResources(AppResourceLoaderImpl.java:371) at com.logpresso.sonar.api.exchange.impl.AppResourceLoaderImpl.importResources(AppResourceLoaderImpl.java) at com.logpresso.sonar.api.exchange.impl.AppServiceImpl.\_\_M\_validateObjects(AppServiceImpl.java:1203) at com.logpresso.sonar.api.exchange.impl.AppServiceImpl.validateObjects(AppServiceImpl.java) at com.logpresso.sonar.api.exchange.impl.AppServiceImpl.\_\_M\_validateInstallableBeforeOverwrite(AppServiceImpl.java:1197) at com.logpresso.sonar.api.exchange.impl.AppServiceImpl.validateInstallableBeforeOverwrite(AppServiceImpl.java) at com.logpresso.sonar.api.exchange.impl.AppServiceImpl.\_\_M\_validateInstallableStatusBeforeOverWrite(AppServiceImpl.java:1249) at com.logpresso.sonar.api.exchange.impl.AppServiceImpl.validateInstallableStatusBeforeOverWrite(AppServiceImpl.java) at com.logpresso.sonar.api.exchange.impl.AppServiceImpl.\_\_M\_startInstallApp(AppServiceImpl.java:478) at com.logpresso.sonar.api.exchange.impl.AppServiceImpl.startInstallApp(AppServiceImpl.java) at com.logpresso.sonar.msgbus.AppPlugin.\_\_M\_startInstallApp(AppPlugin.java:85) at com.logpresso.sonar.msgbus.AppPlugin.startInstallApp(AppPlugin.java) at java.base/jdk.internal.reflect.DirectMethodHandleAccessor.invoke(DirectMethodHandleAccessor.java:103) at java.base/java.lang.reflect.Method.invoke(Method.java:580) at org.araqne.msgbus.handler.MsgbusPluginHandler.\_\_M\_handleMessage(MsgbusPluginHandler.java:197) at org.araqne.msgbus.handler.MsgbusPluginHandler.handleMessage(MsgbusPluginHandler.java) at org.araqne.msgbus.impl.MessageBusImpl$TaskRunner.\_\_M\_invokeMessageHandler(MessageBusImpl.java:591) at org.araqne.msgbus.impl.MessageBusImpl$TaskRunner.invokeMessageHandler(MessageBusImpl.java) at org.araqne.msgbus.impl.MessageBusImpl$TaskRunner.\_\_M\_run(MessageBusImpl.java:580) at org.araqne.msgbus.impl.MessageBusImpl$TaskRunner.run(MessageBusImpl.java) at java.base/java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1144) at java.base/java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:642) at java.base/java.lang.Thread.run(Thread.java:1583)Caused by: org.json.JSONException: A JSONObject text must begin with '{' at character 1 at org.json.JSONTokener.syntaxError(JSONTokener.java:409) at org.json.JSONObject.<init>(JSONObject.java:190) at org.json.JSONObject.<init>(JSONObject.java:423) at com.logpresso.sonar.api.exchange.impl.LoggerModelExchangeServiceImpl.\_\_M\_loadJson(LoggerModelExchangeServiceImpl.java:303) ... 28 more