## 릴리스 3.1.2207.0

### 유의 사항

* araqne-core 버전을 3.8.0으로 업데이트 되었으므로 패치 시 araqne-core도 함께 업데이트해야 합니다.
* 이번 배포 버전부터 로그프레소 서버 구동 시 JDK 11 버전을 사용해야 합니다. 서버용 JDK 11 버전은 [로그프레소 스토어에서 다운로드](https://logpresso.store/ko/packages/jdk/releases) 가능합니다.
* 이번 배포 버전부터 로그프레소 센트리는 JDK 6을 더 이상 지원하지 않으며, JDK 7, 8, 혹은 11 버전을 사용해야 합니다.
* 기존 마리아 DB의 위협 인텔리전스 피드 테이블이 삭제되므로 업그레이드를 실행하기 전에 DB를 백업하세요. 업그레이드 이후에는 위협 인텔리전스 피드 동기화 재설정 작업이 필요합니다. [SNR#1552 릴리스 노트](https://docs.logpresso.com/ko/sonar/3.1/releases/ko/sonar/3.1/issues/SNR1552)를 참고하여 동기화 재설정 CLI 명령어를 수행하세요.
* 패치 후 CLI에서 다음과 같이 web\_endpoint 옵션을 설정해야 티켓 알림 메일 발송 시 "로그프레소에서 보기" 링크가 의도한대로 동작합니다. 신규 설치 시에는 자동으로 web\_endpoint 옵션이 설정됩니다.
* logpresso> sonar.setGlobalOption web\_endpoint https://HOSTNAME

### 신규 기능

|  |  |
| --- | --- |
| 식별자 | 항목 |
| [SNR#1532](https://docs.logpresso.com/ko/sonar/3.1/issues/SNR1532) | 센트리 원격 재시작 및 실시간 정보 조회 기능 추가 |
| [SNR#1552](https://docs.logpresso.com/ko/sonar/3.1/issues/SNR1552) | 앱 인텔리전스 지원 체계 추가 |

### 기능 개선

|  |  |
| --- | --- |
| 식별자 | 항목 |
| [SNR#1095](https://docs.logpresso.com/ko/sonar/3.1/issues/SNR1095) | 메일 설정 및 티켓 메일 양식 개선 |
| [SNR#1492](https://docs.logpresso.com/ko/sonar/3.1/issues/SNR1492) | 웹 서버 TLS 취약점 제거 |
| [SNR#1506](https://docs.logpresso.com/ko/sonar/3.1/issues/SNR1506) | 화면 잠금 기능 개선 |
| [SNR#1687](https://docs.logpresso.com/ko/sonar/3.1/issues/SNR1687) | 계정 잠금 설정 변경 |
| [SNR#1707](https://docs.logpresso.com/ko/sonar/3.1/issues/SNR1707) | 드롭다운 메뉴의 항목 길이에 따라 가로폭이 확장되도록 개선 |
| [SNR#1747](https://docs.logpresso.com/ko/sonar/3.1/issues/SNR1747) | Netty 4 버전 업데이트 |
| [SNR#1749](https://docs.logpresso.com/ko/sonar/3.1/issues/SNR1749) | 경고상자 위젯 불필요한 여백 및 세로 스크롤 제거 |
| [SNR#1750](https://docs.logpresso.com/ko/sonar/3.1/issues/SNR1750) | 쿼리스트링을 이용한 대시보드 입력 변수 설정 지원 |
| [SNR#1751](https://docs.logpresso.com/ko/sonar/3.1/issues/SNR1751) | 위젯 클릭 이벤트에서 GLOBAL\_FILTERS 매크로 지원 |
| [SNR#1752](https://docs.logpresso.com/ko/sonar/3.1/issues/SNR1752) | 위젯 이벤트에 화면 전환 옵션 추가 |
| [SNR#1792](https://docs.logpresso.com/ko/sonar/3.1/issues/SNR1792) | 계정 그룹에 대해 소나 프로시저 권한 부여 지원 |
| [SNR#1809](https://docs.logpresso.com/ko/sonar/3.1/issues/SNR1809) | 탐지 시나리오에 IP 블랙리스트 등록, IP 차단필드 설정 추가 |
| [SNR#1829](https://docs.logpresso.com/ko/sonar/3.1/issues/SNR1829) | 첨부파일 이름 툴팁 지원 |
| [SNR#1845](https://docs.logpresso.com/ko/sonar/3.1/issues/SNR1845) | 소명 제출/반려/승인 후, 스크롤을 최상단으로 이동 |
| [SNR#1856](https://docs.logpresso.com/ko/sonar/3.1/issues/SNR1856) | 시나리오 쿼리 항목을 10000자까지 입력 가능하도록 개선 |
| [SNR#1902](https://docs.logpresso.com/ko/sonar/3.1/issues/SNR1902) | 하둡 관련 모듈 제거 |
| [SNR#1922](https://docs.logpresso.com/ko/sonar/3.1/issues/SNR1922) | 로그프레소 사명 변경 반영 |
| [SNR#1930](https://docs.logpresso.com/ko/sonar/3.1/issues/SNR1930) | dataset 쿼리 커맨드 성능 개선 |

### 버그 해결

|  |  |
| --- | --- |
| 식별자 | 항목 |
| [SNR#1188](https://docs.logpresso.com/ko/sonar/3.1/issues/SNR1188) | 소나 부팅 시 빌드되지 않은 행위 프로파일에 대해 오류가 발생하는 현상 해결 |
| [SNR#1249](https://docs.logpresso.com/ko/sonar/3.1/issues/SNR1249) | 서버 장애 판단 기준을 일정 기간 무응답으로 변경 |
| [SNR#1359](https://docs.logpresso.com/ko/sonar/3.1/issues/SNR1359) | 쿼리 창 문법 강조 개선 - 따옴표 내 괄호 처리, 서브쿼리 내 주석 처리, 둥근 따옴표 문자열 강조 |
| [SNR#1514](https://docs.logpresso.com/ko/sonar/3.1/issues/SNR1514) | 일반 사용자의 사용자 정의 변수 조회 시 다른 사용자의 변수도 조회되는 문제 해결 |
| [SNR#1567](https://docs.logpresso.com/ko/sonar/3.1/issues/SNR1567) | 목록 화면에서 긴 항목이 겹쳐 표시되는 현상 해결 |
| [SNR#1585](https://docs.logpresso.com/ko/sonar/3.1/issues/SNR1585) | 셸 명령어 sonar.createStreamRule로 룰 생성이 불가능한 문제 해결 |
| [SNR#1595](https://docs.logpresso.com/ko/sonar/3.1/issues/SNR1595) | 쿼리 자동 완성 시 쿼리 명령어와 옵션을 구분하지 않는 문제 해결 |
| [SNR#1623](https://docs.logpresso.com/ko/sonar/3.1/issues/SNR1623) | 대시보드 레이아웃 편집 후 위젯 크기 변경이 되지 않는 문제 해결 |
| [SNR#1700](https://docs.logpresso.com/ko/sonar/3.1/issues/SNR1700) | 접속 프로파일 동기화 트레이스에서 암호 평문이 노출되는 문제 해결 |
| [SNR#1705](https://docs.logpresso.com/ko/sonar/3.1/issues/SNR1705) | 클러스터 관리자에게 IP 분류가 중복 표시되는 문제 해결 |
| [SNR#1709](https://docs.logpresso.com/ko/sonar/3.1/issues/SNR1709) | 피벗 메뉴에서 컬럼을 값, 행, 열 항목에 드래그 할 때 쿼리가 실행되지 않는 현상 해결 |
| [SNR#1711](https://docs.logpresso.com/ko/sonar/3.1/issues/SNR1711) | 위젯 동적 필터의 사용자 지정 변수 이름을 문자열이 아닌 map 타입으로 저장되는 현상 수정 |
| [SNR#1740](https://docs.logpresso.com/ko/sonar/3.1/issues/SNR1740) | 차트 클릭 이벤트로 쿼리 실행 시 매크로가 치환되지 않는 현상 해결 |
| [SNR#1746](https://docs.logpresso.com/ko/sonar/3.1/issues/SNR1746) | 다른 창이나 탭에서 로그인 후 새로고침 했을 때 첫 화면에서 로그인 창이 보이는 현상 해결 |
| [SNR#1774](https://docs.logpresso.com/ko/sonar/3.1/issues/SNR1774) | 정규화 메뉴에서 스키마 목록을 불러오기 전에 다른 페이지로 이동할 경우 다시 정규화 메뉴로 돌아가는 문제 해결 |
| [SNR#1819](https://docs.logpresso.com/ko/sonar/3.1/issues/SNR1819) | SNMP 트랩 수집기 삭제 후 동일 설정으로 다시 생성 시 실패하는 현상 해결 |
| [SNR#1921](https://docs.logpresso.com/ko/sonar/3.1/issues/SNR1921) | 소나 Angular SDK의 웹소켓 초기화 오류로 인해 앱이 반복적으로 웹소켓 접속을 시도하는 현상 해결 |

### 상세 내역

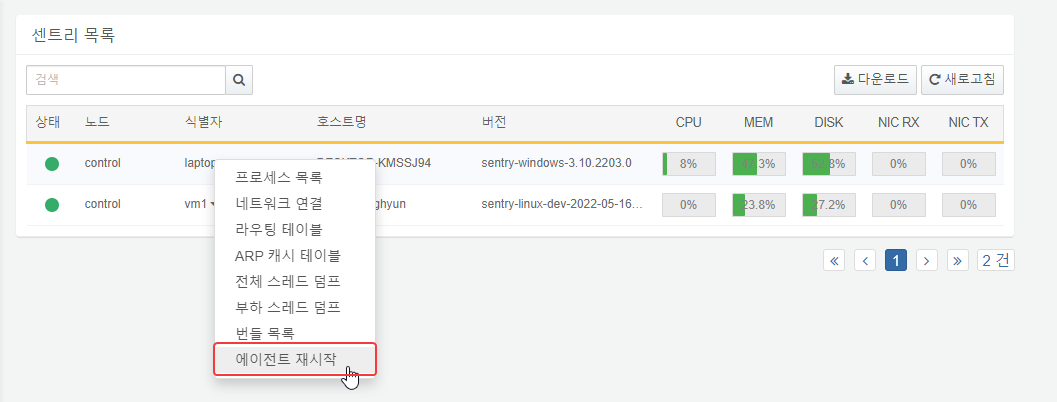
#### SNR#1532 센트리 원격 재시작 및 실시간 정보 조회 기능 추가

아래의 기능을 추가했습니다.

* 센트리 원격 재시작
* 센트리 실시간 정보 조회
* 센트리 실시간 쿼리 명령어

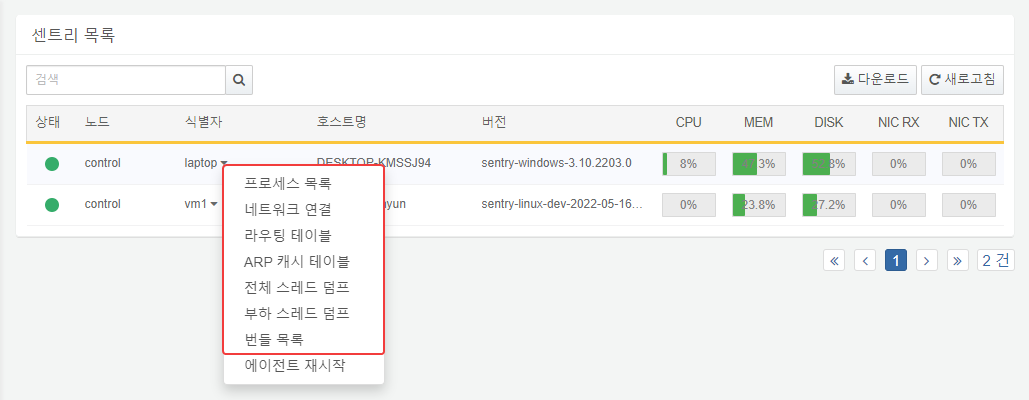
**센트리 원격 재시작**

센트리 원격 재시작 기능을 추가했습니다. 웹 관리화면에서 센트리를 원격으로 재시작할 수 있습니다.



**센트리 실시간 정보 조회**

센트리의 프로세스 목록, 네트워크 연결, 라우팅 테이블, ARP 캐시 테이블, 전체 스레드 덤프, 부하 스레드 덤프, 번들 목록 등 실시간 정보를 조회하는 기능을 추가했습니다.



**센트리 실시간 쿼리 명령어**

서버에서 센트리 목록 및 센트리의 프로세스 목록, 네트워크 연결, 라우팅 테이블, ARP 캐시 테이블, 전체 스레드 덤프, 부하 스레드 덤프, 번들 목록, 수집기 목록, 수집기 설정 등 정보를 조회하는 쿼리 명령어를 추가했습니다.

* sonar-sentries [guids=센트리GUID목록] [timeout=타임아웃] : 등록된 모든 센트리 목록 조회
* sonar-sentry-processes [guids=센트리GUID목록] [timeout=타임아웃] : 센트리 프로세스 목록 조회
* sonar-sentry-netstat [guids=센트리GUID목록] [timeout=타임아웃] : 센트리 네트워크 연결 목록 조회
* sonar-sentry-routing-table [guids=센트리GUID목록] [timeout=타임아웃] : 센트리 라우팅 테이블 조회
* sonar-sentry-arp-cache [guids=센트리GUID목록] [timeout=타임아웃] : 센트리 ARP 캐시 테이블 조회
* sonar-sentry-jstack [guids=센트리GUID목록] [timeout=타임아웃] : 센트리 전체 스레드 덤프 조회
* sonar-sentry-top-threads [guids=센트리GUID목록] [timeout=타임아웃] : 센트리 부하 스레드 덤프 조회
* sonar-sentry-bundles [guids=센트리GUID목록] [timeout=타임아웃] : 센트리 번들 목록 조회
* sonar-sentry-loggers [guids=센트리GUID목록] [timeout=타임아웃] : 센트리 전체 수집기 목록 조회
* sonar-sentry-logger-configs [guids=센트리GUID목록] [timeout=타임아웃] : 센트리 전체 수집기 설정 조회

#### SNR#1552 앱 인텔리전스 지원 체계 추가

아래의 기능을 추가했습니다.

* 위협 인텔리전스 피드 저장 방식 변경 및 확장 기능 추가
* matchfeed, node-feed 커맨드에 type 옵션 추가
* matchioc() 함수 추가
* 실시간 시나리오 템플릿 추가/변경
* CLI 명령어 추가
* sonar.resetThreatFeed
* sonar.resetNodeSyncStatus
* CLI 명령어 제거
* sonar.isacKey
* sonar.setIsacKey

위협 인텔리전스 피드 확장 기능 추가

앱 설치를 통해 위협 인텔리전스 피드를 확장하는 기능이 추가되었습니다. 이에 따라 다양한 데이터 스키마를 수용할 수 있도록 위협 인텔리전스 피드를 로그프레소 테이블에 저장합니다. 마이그레이션 시, **기존 마리아DB의 위협 인텔리전스 피드 테이블이 삭제**됩니다.

위협 인텔리전스 피드 확장 기능을 포함한 앱을 설치하면, **sonar\_ioc\_** 접두어로 시작하는 로그프레소 테이블을 생성하고 피드 데이터를 저장합니다.

matchfeed, node-feed 커맨드에 type 옵션 추가

matchfeed, node-feed 커맨드에 type 옵션이 추가되었습니다. name 옵션과 type 옵션을 함께 사용하는 경우, type 옵션이 무시됩니다.

matchfeed [fields=대상필드목록] [invert=t|f] [name=피드이름] [type=피드타입]

**사용 예**

* matchfeed fields=src\_ip name=otx
* src\_ip 필드 값을 **otx 피드**와 매칭
* matchfeed fields=src\_ip type=ip
* src\_ip 필드 값을 **모든 IP 타입의 피드**와 매칭

node-feed [name=피드이름] [type=피드타입]

matchioc() 함수 추가

특정 침해지표 유형의 모든 피드에서 값을 검색하는 함수를 추가했습니다.

matchioc(FEED\_TYPE, EXPR)

**반환 값**

FEED\_TYPE 타입의 피드 중에서 EXPR 값이 검색되면 true, 검색되지 않으면 false

실시간 시나리오 템플릿 추가 및 변경

실시간 시나리오 템플릿을 추가 및 변경했습니다. 항목은 아래와 같습니다.

* 룰 템플릿 추가
* IP 주소가 평판 DB에 포함
* MD5가 특정 평판 DB에 포함
* URL이 평판 DB에 포함
* URL이 특정 평판 DB에 포함
* 룰 이름 변경
* PE 블랙리스트에 포함 -> 대상 해시값과 일치
* PE 평판 DB에 포함 -> MD5가 평판 DB에 포함
* IP 주소가 IP 평판 DB에 포함 -> IP 주소가 특정 평판 DB에 포함

**CLI 명령어 추가**

모든 노드의 위협 인텔리전스 피드 동기화 상태를 초기화하는 CLI 명령어와 특정 노드의 피드 동기화 상태를 초기화하는 CLI 명령어를 추가했습니다.

sonar.resetThreatFeed 피드이름 수집기준날짜 [수집기준ID]

* 모든 노드에서 지정된 위협 인텔리전스 피드의 모든 데이터를 삭제하고 입력한 기준 날짜부터 다시 수집합니다.
* 예시: sonar.resetThreatFeed otx 20180101
* otx 피드 데이터를 초기화하고 2018-01-01부터 수집하도록 기준 날짜를 재설정합니다.

sonar.resetNodeSyncStatus 피드이름 노드GUID 동기화기준날짜 [동기화기준ID]

* 특정 노드에 동기화된 위협 인텔리전스 피드 데이터를 삭제하고 입력한 기준 날짜부터 다시 수집합니다.
* 예시: sonar.resetNodeSyncStatus malc0de abc8777c-c6de-4949-bec4-f31a63ee5ffc 20170818
* 지정된 노드에 동기화된 malc0de 피드의 모든 데이터를 삭제하고 2017-08-18부터 수집하도록 동기화 기준 날짜를 재설정합니다.

**CLI 명령어 제거**

기존에 존재하던 ISAC KEY 등록/조회 관련 CLI 명령어가 제거되었습니다.

sonar.isacKeysonar.setIsacKey ISAC\_API\_KEY

ISAC KEY 관련 등록/조회는 SONAR Global Options 관련 CLI 명령어로 가능합니다.

sonar.globalOptions isac\_api\_keysonar.setGlobalOptions isac\_api\_key ISAC\_API\_KEY

#### SNR#1095 메일 설정 및 티켓 메일 양식 개선

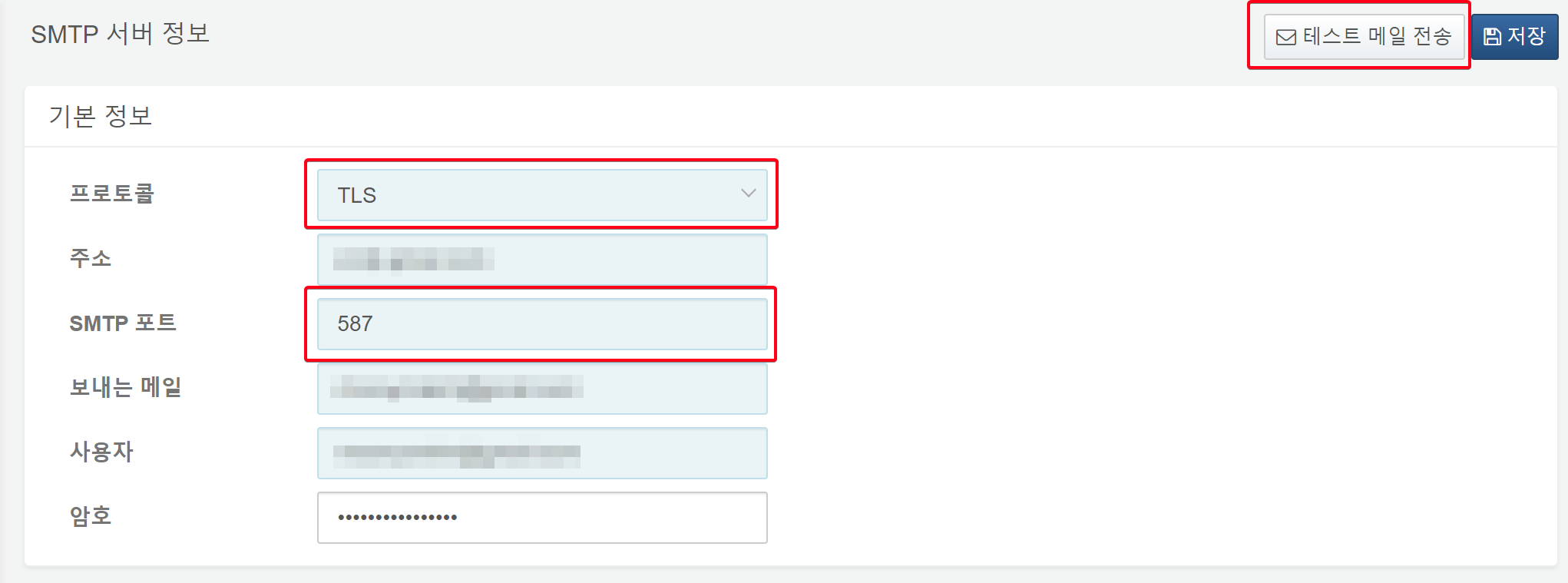
웹 인스톨러 기능을 개선했습니다.

* 서버 웹 주소 설정 기능 추가
* 클러스터 관리자 언어 설정 기능 추가

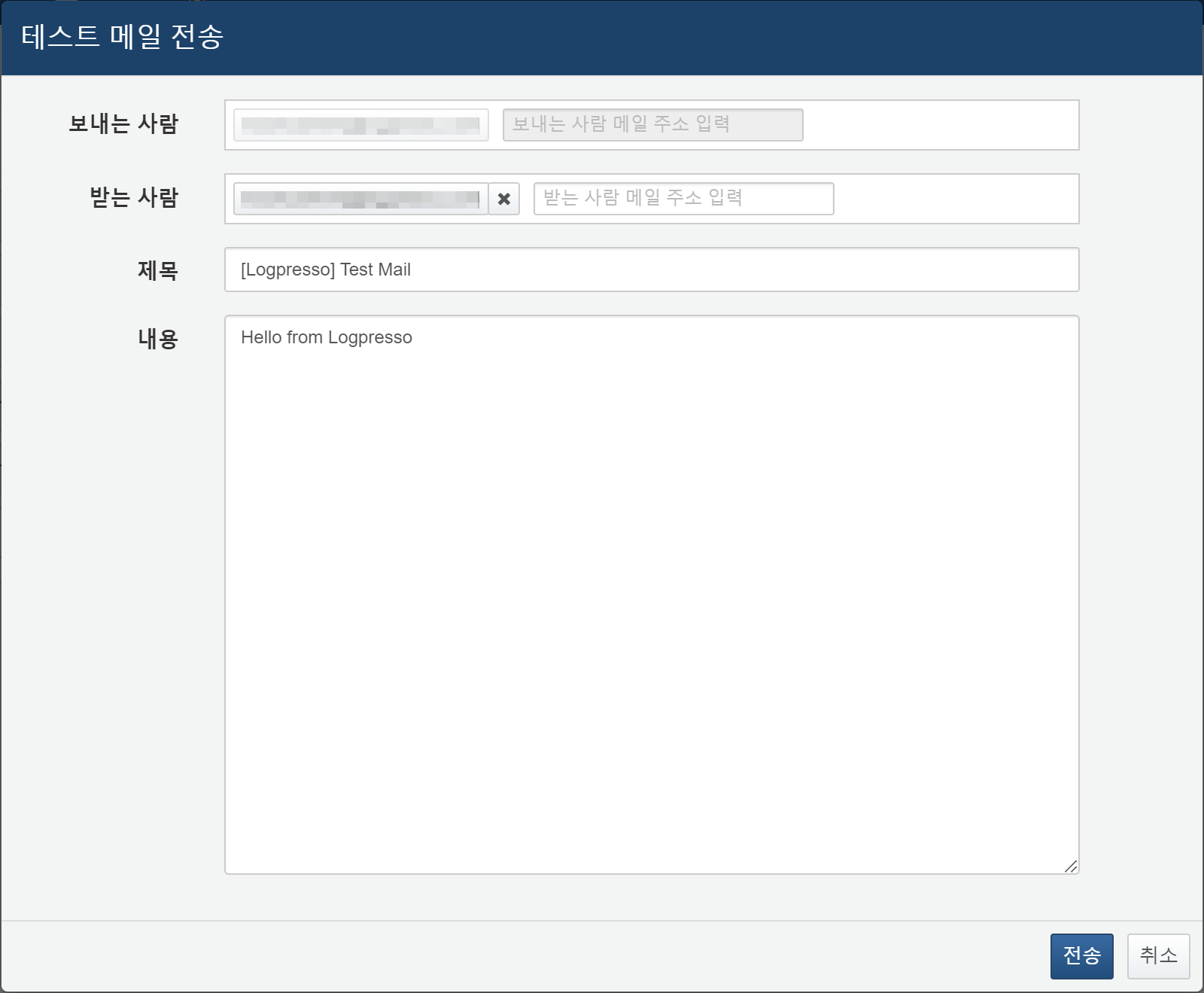


메일 서버 설정 화면을 개선했습니다.

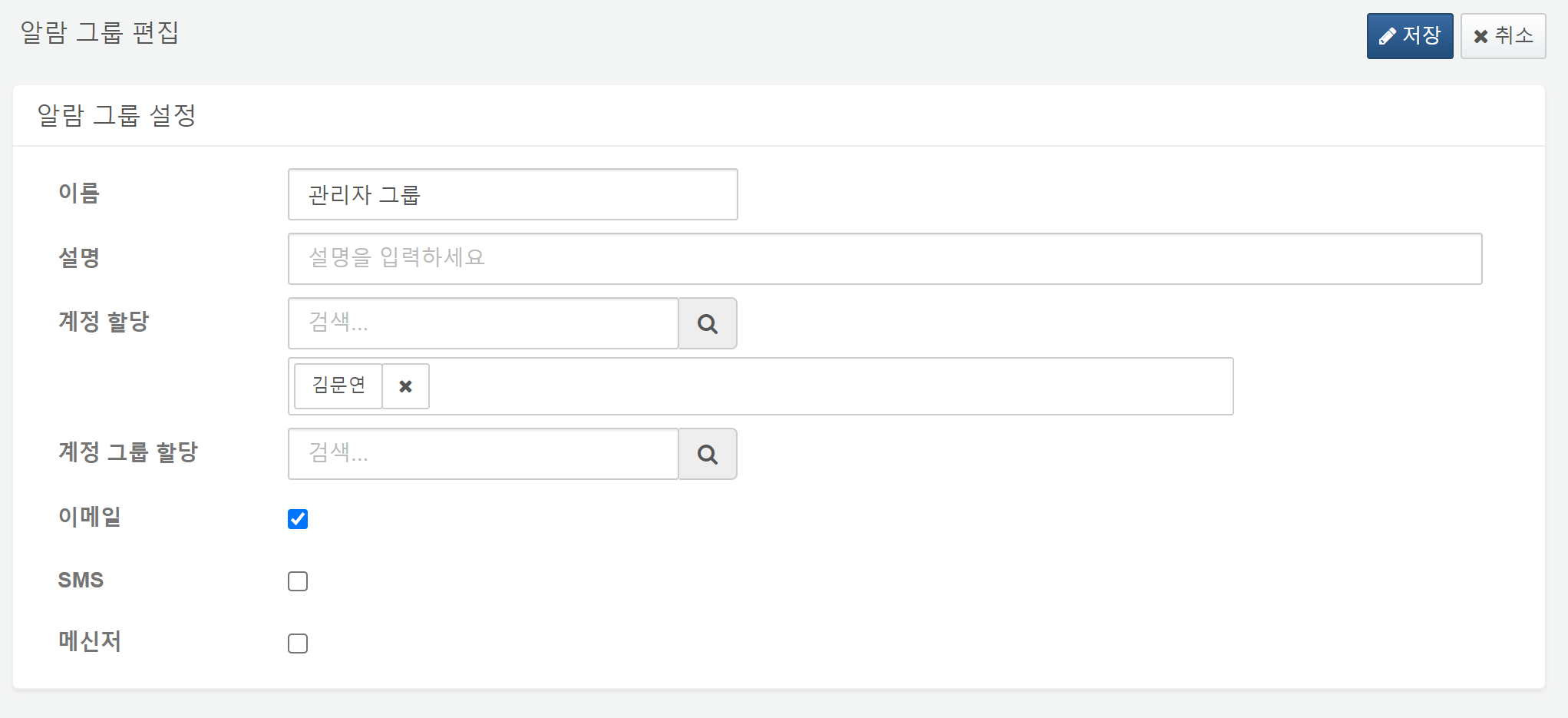
* 프로토콜 기본값을 TLS로 설정
* SMTP포트 기본값을 587로 설정
* 테스트 메일 전송 버튼 추가



"테스트 메일 전송" 버튼 클릭 시 테스트 메일 전송 화면이 표시됩니다.



최초 설치 시 관리자 그룹이 자동 생성되며 이메일 알림 기능이 설정되어 있습니다.시나리오 생성 시 알림 그룹에 관리자 그룹을 지정할 경우 이메일 알림이 발송됩니다.



티켓 알람 그룹을 지정한 경우 별도로 ENT 스트림 쿼리를 수정하지 않아도 메일이 전송되도록 개선되었습니다.

패치 후 CLI에서 다음과 같이 web\_endpoint 옵션을 설정해야 티켓 알림 메일 발송 시 "로그프레소에서 보기" 링크가 의도한대로 동작합니다. 신규 설치 시에는 자동으로 web\_endpoint 옵션이 설정됩니다.

logpresso> sonar.setGlobalOption web\_endpoint https://HOSTNAME

패치 전 : 관리자가 직접 ENT UI에서 스트림 쿼리를 수정하여 티켓 알림 메일 전송 (본문에 message만 나오게 설정한 결과)



패치 후 : 티켓 알림 메일 기본 발송



#### SNR#1492 웹 서버 TLS 취약점 제거

* TLS1, TLS1.1가 기본으로 비활성화 됩니다. 해당 TLS 버전 활성화가 필요한 경우 부팅 옵션에 -Daraqne.httpd.weak\_tls=enabled 를 추가해야 합니다.
* CBC, DH suite가 기본으로 비활성화 됩니다. 해당 suite 활성화가 필요한 경우 부팅 옵션에 -Daraqne.httpd.weak\_cipher=enabled 를 추가해야 합니다.
* TLS 접속 시 2048 비트 이상의 DH 그룹으로 강제하여 LOGJAM ([CVE-2015-4000](https://github.com/advisories/GHSA-v98w-p8f7-9qqf)) 취약점을 해결했습니다.
* TLS 접속 시 CBC 암호화를 금지하여 LUCKY13 ([CVE-2013-0169](https://github.com/advisories/GHSA-pg96-42c4-p633)) 취약점을 해결했습니다.

#### SNR#1506 화면 잠금 기능 개선

화면 잠금 시 배경에 기존 화면 내용이 표시되지 않도록 개선했습니다.

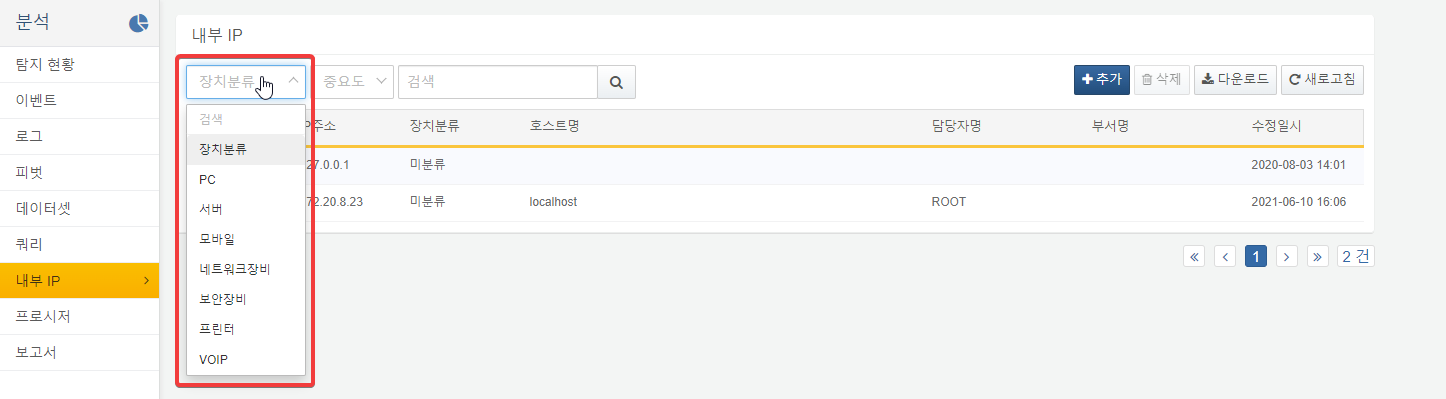
#### SNR#1687 계정 잠금 설정 변경

계정 잠금 설정 시 다음 내용이 변경했습니다.

* 최대 로그인 실패 횟수는 5회를 초과할 수 없음
* 신뢰하는 호스트 설정 시 127.0.0.1 이나 ::1 을 입력하지 않아도 로컬에서 접속 허용

#### SNR#1707 드롭다운 메뉴의 항목 길이에 따라 가로폭이 확장되도록 개선

실시간 탐지 시나리오 메뉴의 분류, 탐지 현황 메뉴의 분류, 임직원 메뉴의 분류, 내부 IP 메뉴의 장치 분류 드롭다운 항목을 표시할 때 항목이 ... 으로 생략되지 않고 전체가 표시되도록 수정했습니다.

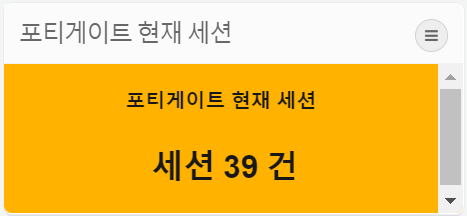
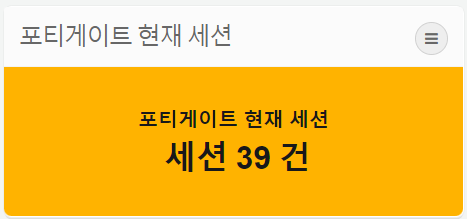


#### SNR#1747 Netty 4 버전 업데이트

Netty 버전을 3.10.4.Final에서 4.1.75.Final로 업데이트 했습니다.

#### SNR#1749 경고상자 위젯의 불필요한 여백 및 세로 스크롤 제거

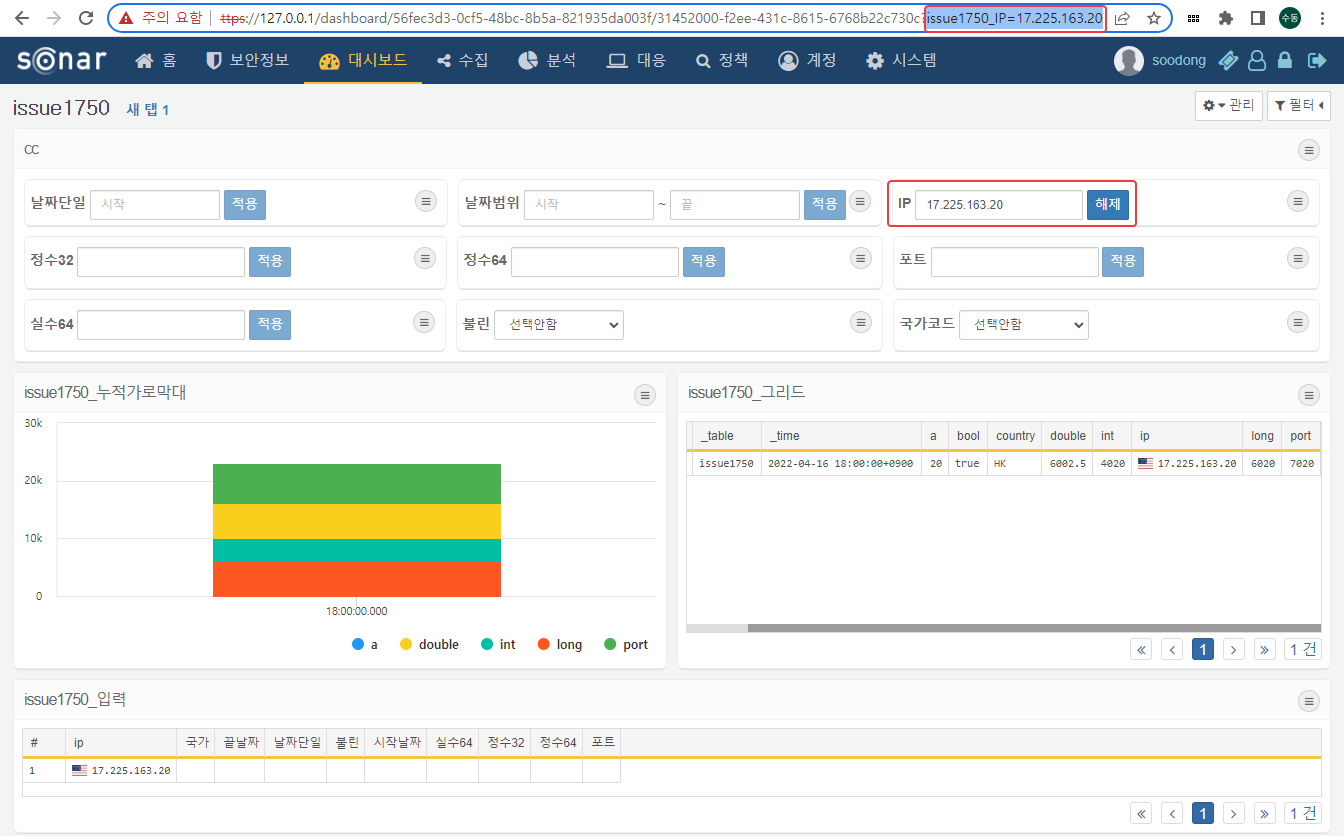
경고상자 위젯에서 라벨이 없는 경우에 빈 영역을 표시하지 않고 내용을 중앙 정렬하도록 변경했습니다. 또한 위젯 가로폭이 충분한 경우 불필요한 세로 스크롤을 표시하지 않도록 변경했습니다.

* 패치 전 : 불필요한 여백 및 스크롤바 표시
* 패치 후 : 불필요한 여백 및 스크롤바 제거

#### SNR#1750 쿼리스트링을 이용한 대시보드 입력 변수 설정 지원

대시보드 쿼리스트링에 입력 변수를 지정하면, 페이지 로드 시 입력 변수를 설정하여 입력 컨트롤 위젯에 반영합니다.

아래는 대시보드 URL에 ?issue1750\_IP=17.225.163.20 으로 쿼리스트링을 지정한 경우, 대시보드를 불러오는 시점에 자동으로 IP 입력 컨트롤 위젯의 입력 변수 값이 17.225.163.20 으로 설정되는 동작 예시입니다.



#### SNR#1751 위젯 클릭 이벤트에서 GLOBAL\_FILTERS 매크로 지원

위젯 클릭 이벤트에서 드릴다운 조건을 반영할 수 있도록 $GLOBAL\_FILTERS$ 매크로를 추가했습니다.

위젯 클릭 이벤트 쿼리 세팅 예시

proc vpn\_use\_time() $GLOBAL\_FILETERS

필터 미적용 상태에서 클릭 이벤트 발생 시 실행 쿼리

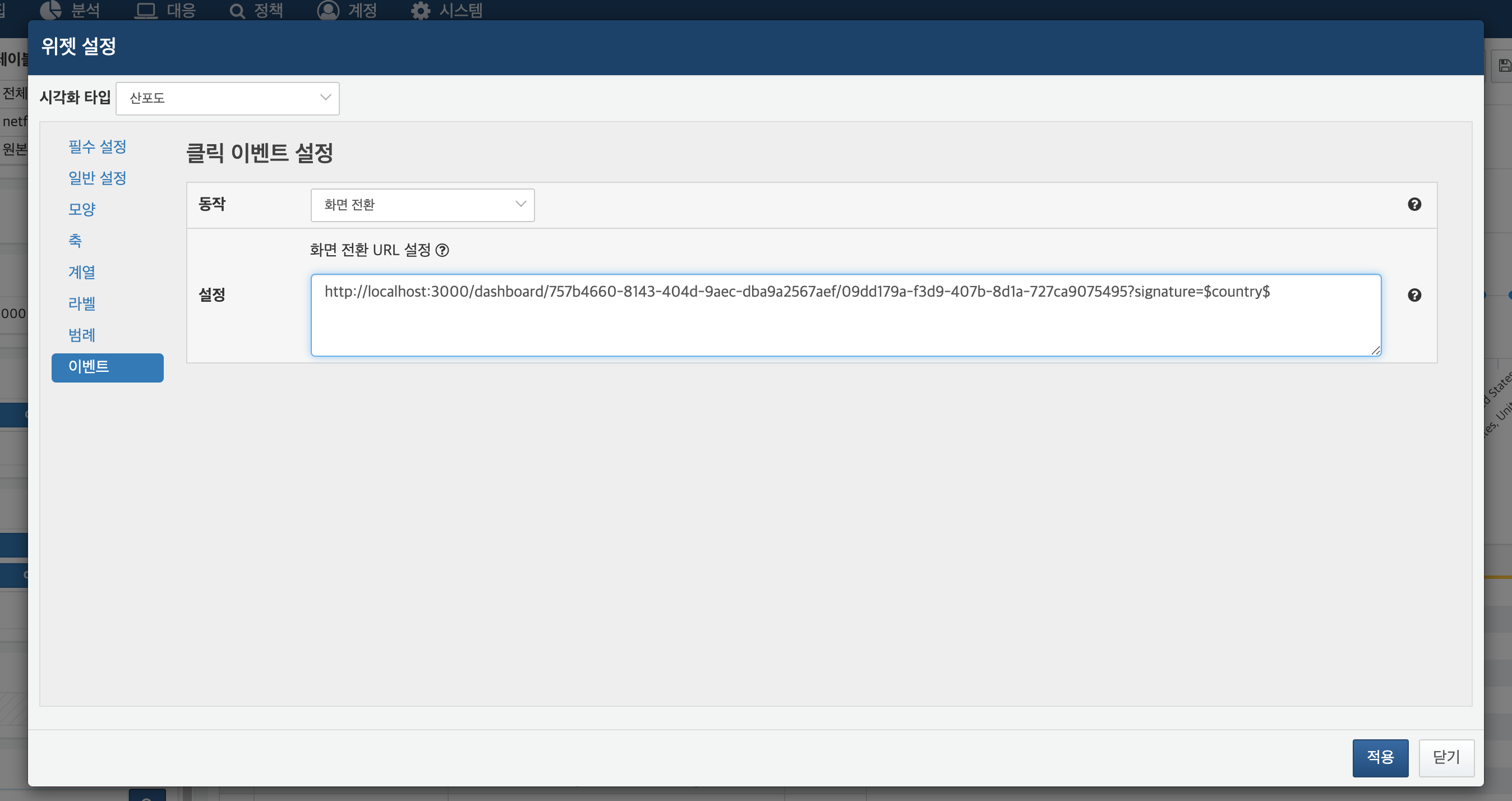
proc vpn\_use\_time()

필터 적용 상태에서 클릭 이벤트 발생 시 쿼리 - 파이프와 search 커맨드 추가

proc vpn\_use\_time()| search emp\_name == "홍길동"| search emp\_title == "과장"

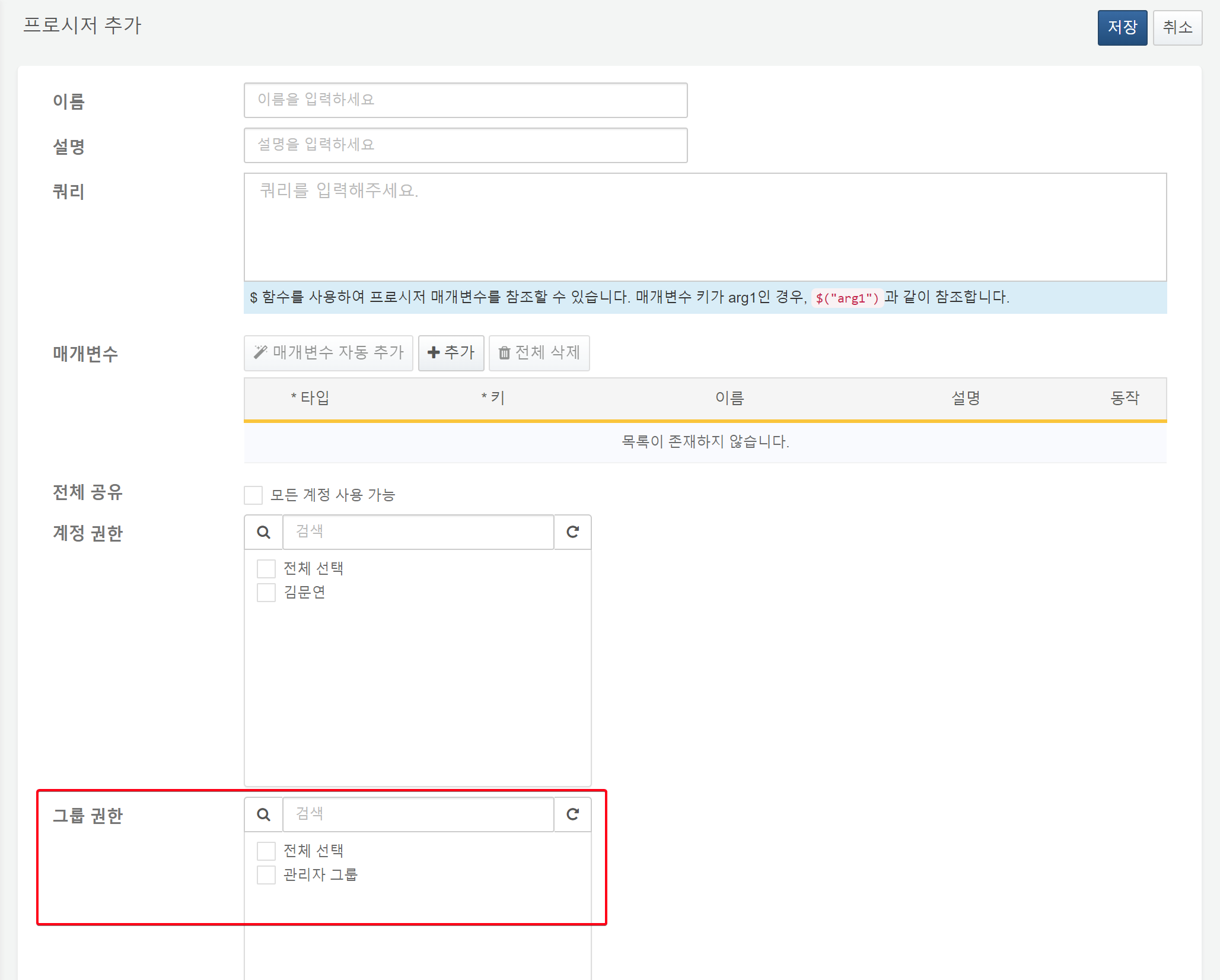
#### SNR#1752 위젯 이벤트에 화면 전환 옵션 추가

위젯 이벤트 발생 시 현재 브라우저 탭을 다른 화면으로 전환하는 옵션을 추가했습니다.



#### SNR#1792 계정 그룹에 대해 소나 프로시저 권한 부여 지원

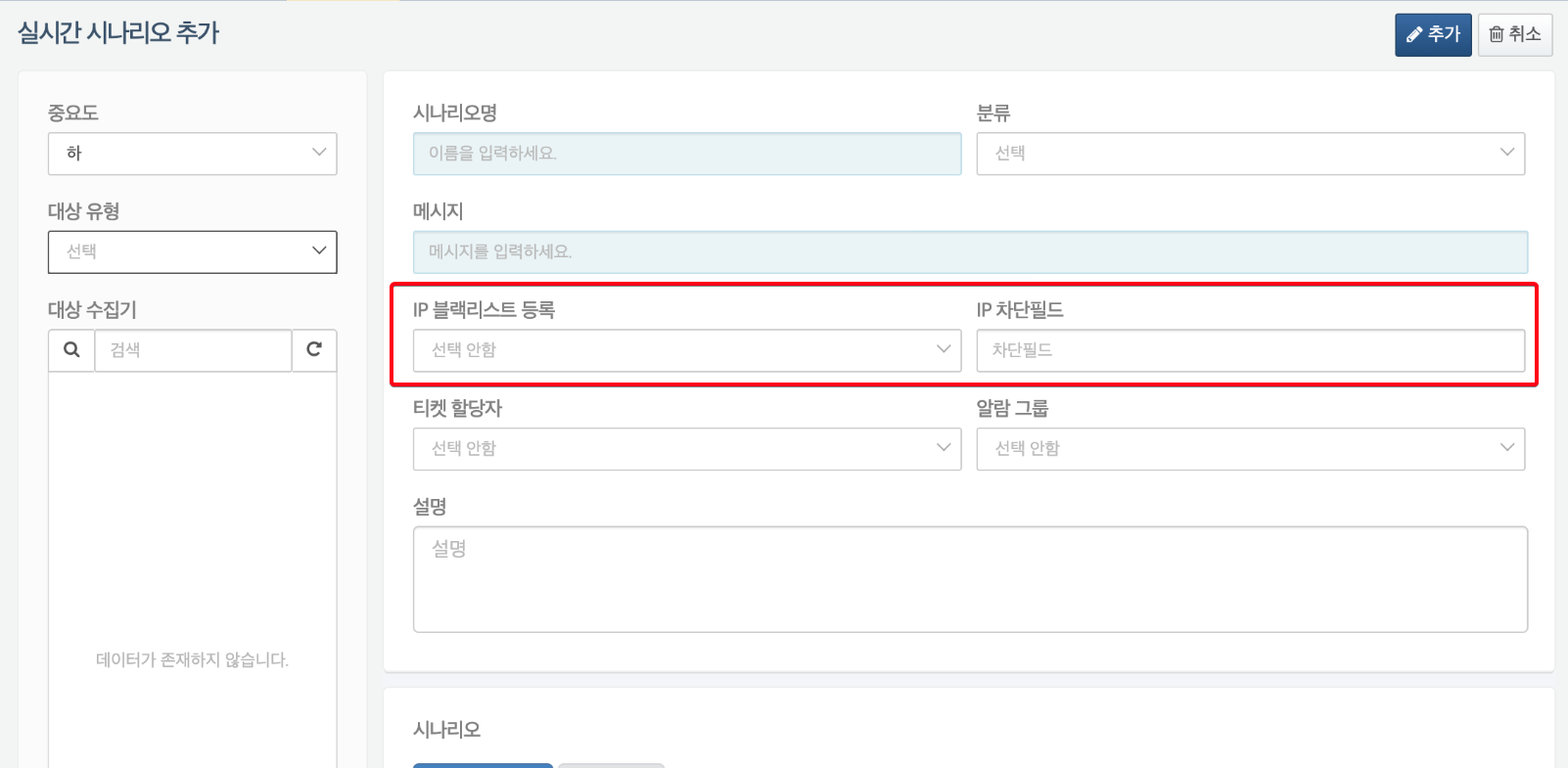
계정 그룹에 대해 프로시저 권한을 지정할 수 있는 기능을 추가했습니다.



#### SNR#1809 탐지 시나리오에 IP 블랙리스트 등록, IP 차단필드 설정 추가

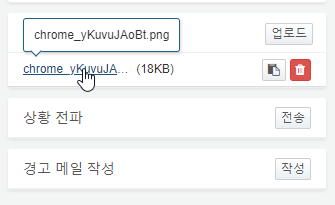
실시간, 배치 탐지 시나리오 설정에 IP 블랙리스트 등록, IP 차단필드 항목을 추가했습니다. 지정한 IP 필드의 값을 IP 블랙리스트에 등록합니다.

* IP 블랙리스트를 선택하지 않으면 IP 주소가 블랙리스트에 등록되지 않습니다.
* IP 블랙리스트를 선택하고 IP 차단필드를 설정하지 않으면 src\_ip 필드가 블랙리스트에 등록됩니다.



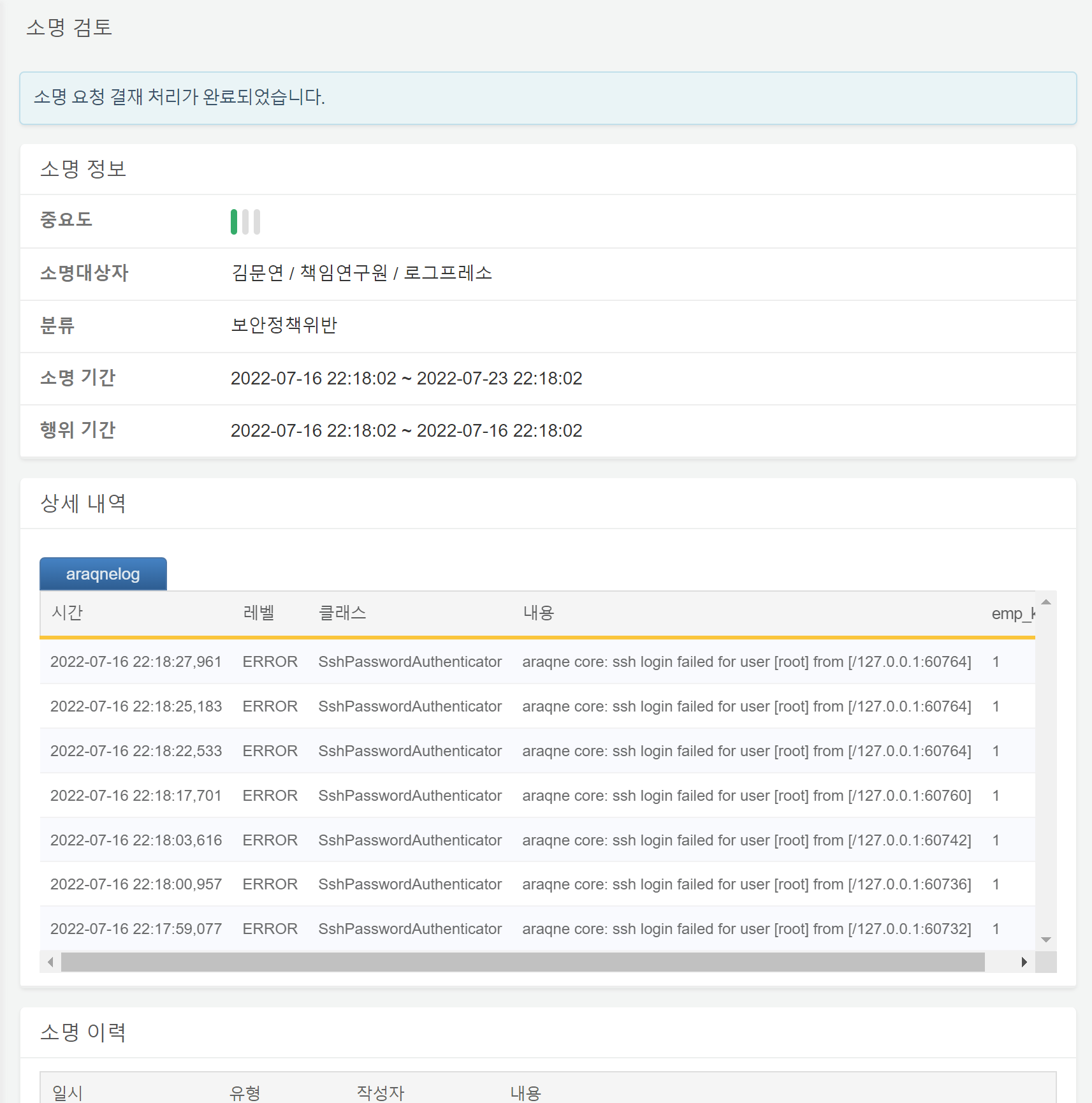
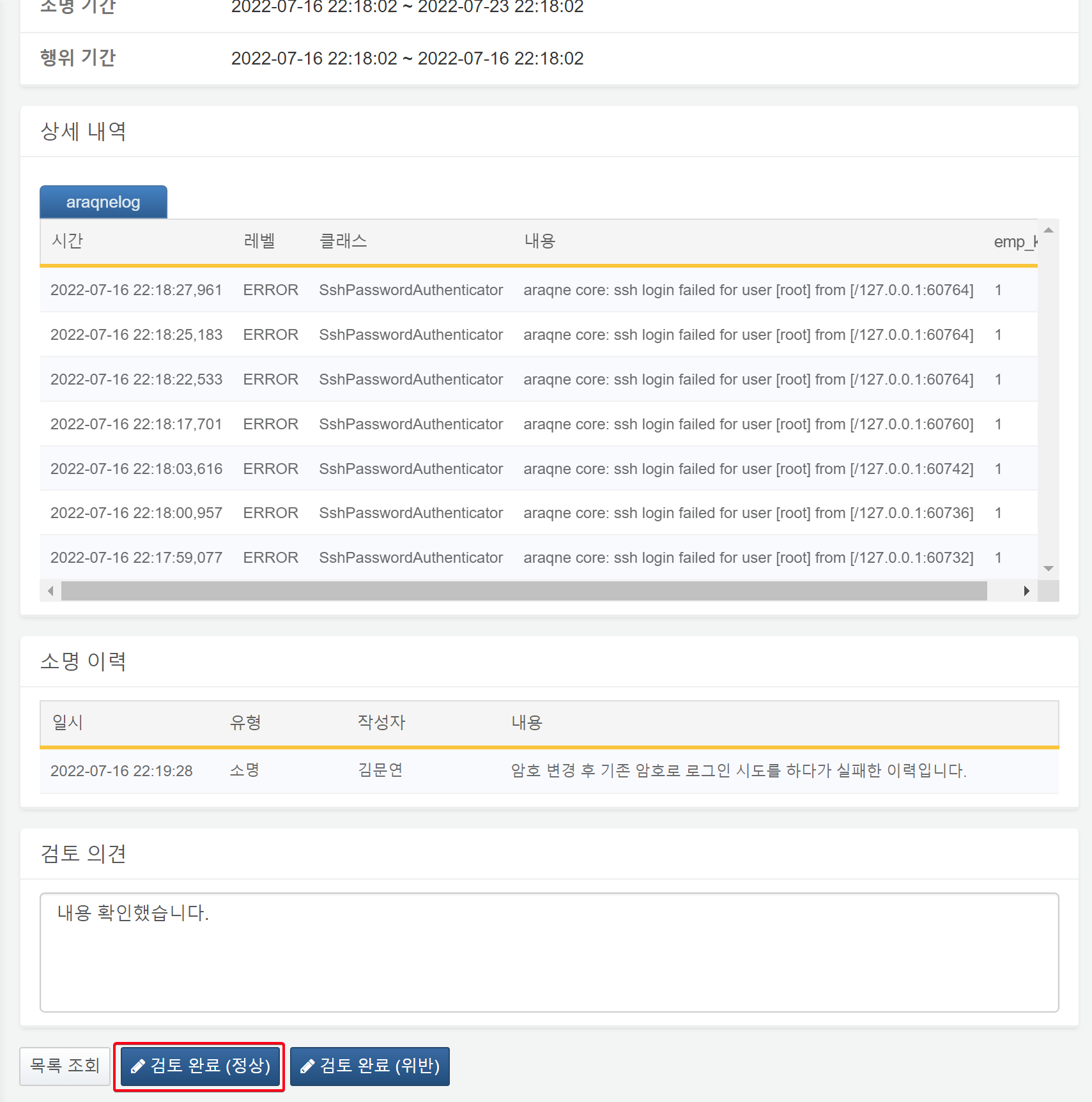
#### SNR#1829 첨부파일 이름 툴팁 지원

첨부파일 이름 위에 마우스 커서를 가져갈 경우 툴팁으로 파일 이름이 표시됩니다. 이름이 길어서 전체가 표시되지 않던 파일 이름을 확인할 수 있습니다.



#### SNR#1845 소명 제출/반려/승인 후, 스크롤을 최상단으로 이동

소명 화면에서 제출/반려/승인 후에 화면 최상단으로 이동합니다.아래와 같이 근거 로그와 소명 이력이 많아 화면 내용이 많을 경우, 제출/반려/승인 버튼 클릭 시 해당 소명 화면의 최상단으로 이동합니다.



#### SNR#1856 시나리오 쿼리 항목을 10000자까지 입력 가능하도록 개선

시나리오 쿼리 입력 제한을 총 10000자로 늘렸습니다. 직접 쿼리를 입력하는 경우 모든 쿼리문 길이의 합을 10000자로 제한합니다.



#### SNR#1902 하둡 관련 모듈 제거

다음 하둡 관련 모듈을 제거했습니다. 추후 하둡 쿼리 및 수집을 하려면 별도 하둡 앱을 설치해야 합니다. (로그프레소 스토어에 공개 예정)

* org.apache.hadoop.client 2.8.0
* org.araqne.storage.hdfs 0.2.2
* com.logpresso.hdfs 1.11.6

#### SNR#1922 로그프레소 사명 변경 반영

구 사명(이디엄)이 표시되던 UI를 수정했습니다.

#### SNR#1930 dataset 쿼리 커맨드 성능 개선

[dataset](https://docs.logpresso.com/ko/query/dataset-command) 쿼리 커맨드를 벡터화하여 기존 배포 버전 대비 통계 수행 성능을 8배 개선했습니다.

#### SNR#1188 소나 부팅 시 빌드되지 않은 행위 프로파일에 대해 오류가 발생하는 현상 해결

부팅 시 빌드되지 않은 행위 프로파일에 대해 불필요한 오류 로그가 발생하던 현상을 해결했습니다. 이전 버전은 아래와 같은 오류 로그가 발생합니다.

[2019-08-02 10:22:26,816] ERROR (BehaviorProfileRegistryImpl) - sonar node: cannot load behavior profile a1ad3370-70ad-43db-94df-882119c04995

#### SNR#1249 서버 장애 판단 기준을 일정 기간 무응답으로 변경

이전에는 소나 서비스에서 다른 노드의 장애 여부를 마지막 하트비트 패킷 응답 여부로 판단했습니다. 다른 노드가 GC 등 여러가지 원인으로 늦게 응답하면, 하트비트 응답이 타임아웃 되면서 장애 판정되어 실제로는 장애가 아닌데도 불필요하게 절체 동작이 발생합니다.

따라서 지정된 기간 이상 (기본값 60초) 하트비트 패킷에 응답하지 않은 경우에 장애로 판정하도록 변경하여 불필요한 장애 절체가 발생하지 않도록 개선하였습니다.

#### SNR#1359 쿼리 창 문법 강조 개선 - 따옴표 내 괄호 처리, 서브쿼리 내 주석 처리, 둥근 따옴표 문자열 강조

쿼리 창에서 일부 문법 강조가 제대로 적용되지 않던 문제를 해결했습니다.

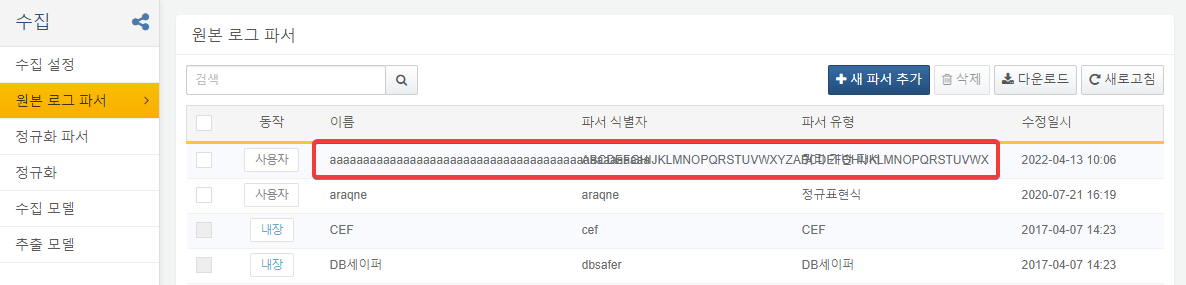
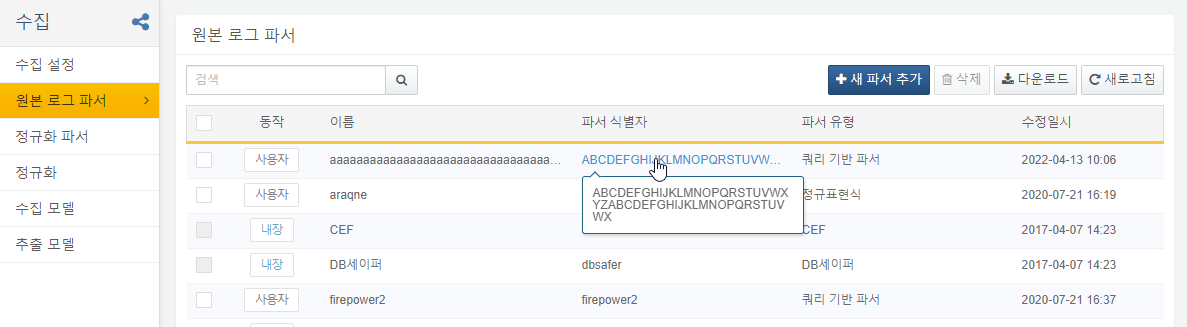
* 따옴표 내 괄호가 있는 경우, 이어지는 명령어들이 문법 강조되지 않던 현상 해결
* 서브쿼리 내에 주석이 있는 경우, 파이프 뒤 쿼리문도 주석 처리된 것처럼 보이던 현상 해결
* 둥근 따옴표(“”)로 묶인 문자열도 문법 강조 처리

#### SNR#1514 일반 사용자의 사용자 정의 변수 조회 시 다른 사용자의 변수도 조회되는 문제 해결

일반 사용자는 다른 사용자의 사용자 정의 변수를 조회할 수 없도록 수정했습니다.

#### SNR#1567 목록 화면에서 긴 항목이 겹쳐 표시되는 현상 해결

UI 목록 화면에서 이름 등 긴 항목이 있을 경우 다른 항목 위에 겹쳐서 표시되던 현상을 해결했습니다. 긴 항목은 축약 표시하며, 마우스 커서를 항목 위에 올리면 툴팁으로 전체 텍스트를 표시합니다.

* 패치 전 - 이름, 파서 식별자, 파서 유형 텍스트가 겹쳐서 표시됨
* 패치 후 - 긴 항목은 축약 표시되고 마우스 커서를 올리면 툴팁으로 전체 텍스트 표시

#### SNR#1585 셸 명령어 sonar.createStreamRule로 룰 생성이 불가능한 문제 해결

sonar.createStreamRule 셸 명령어 실행 시 실시간 탐지 시나리오가 생성되지 않고 아래와 같은 오류가 발생하던 현상을 해결했습니다.

java.lang.IllegalStateException: cannot create empty commmand rule

#### SNR#1595 쿼리 자동 완성 시 쿼리 명령어와 옵션을 구분하지 않는 문제 해결

쿼리 창에서 자동 완성 기능을 사용할 때 쿼리 명령어와 옵션을 구분하지 못하고 도움말 정보를 가져오는 문제를 해결했습니다. fields, order처럼 동일한 이름의 쿼리 명령어와 옵션이 모두 존재하는 경우 문제가 발생합니다.

#### SNR#1623 대시보드 레이아웃 편집 후 위젯 크기 변경이 되지 않는 문제 해결

대시보드 레이아웃을 변경한 이후 위젯 크기 변경이 되지 않는 문제를 해결했습니다.

#### SNR#1700 접속 프로파일 동기화 트레이스에서 암호 평문이 노출되는 문제 해결

로그프레소 셸에서 sonar.traceSync 명령어 사용 시 접속 프로파일 암호가 노출되는 문제를 해결했습니다.

#### SNR#1705 클러스터 관리자에게 IP 분류가 중복 표시되는 문제 해결

클러스터 관리자에게 모든 회사의 IP 카테고리가 중복 표시되는 현상을 해결했습니다. 클러스터 관리자에게는 본인이 속한 기관의 IP 분류만 표시합니다.

#### SNR#1709 피벗 메뉴에서 컬럼을 값, 행, 열 항목에 드래그 할 때 쿼리가 실행되지 않는 현상 해결

피벗 메뉴에서 값, 행, 열 항목에 있는 컬럼을 드래그해서 이동할 때 쿼리가 실행되지 않고 기존 쿼리 결과가 그대로 표시되던 현상을 해결했습니다. 값 항목에 개수(count) 필드가 있는 경우 이를 행이나 열 항목으로 드래그 할 수 없도록 수정했습니다.

#### SNR#1711 위젯 동적 필터의 사용자 지정 변수 이름을 문자열이 아닌 map 타입으로 저장하는 현상 수정

위젯에 적용된 동적 필터의 사용자 지정 변수 이름을 map 타입으로 잘못 저장하는 현상을 수정했습니다.

#### SNR#1740 차트 클릭 이벤트로 쿼리 실행 시 매크로가 치환되지 않는 현상 해결

차트 위젯의 클릭 이벤트로 쿼리 실행 동작을 설정한 경우, 매크로 값들이 타입에 따라 적절하게 치환되지 않던 현상을 해결했습니다.

#### SNR#1746 로그인 상태에서도 페이지 새로고침 시 로그인 입력 창이 보이는 현상 해결

여러 개의 브라우저 창이나 탭에 소나 페이지를 열어둔 상태에서 하나의 창 또는 탭에서 로그인하고 화면을 새로고침 했을때, 이미 로그인이 된 상태인데도 불구하고 자동 로그인이 수행되지 않고 인증 화면을 출력하는 현상을 해결했습니다.

#### SNR#1774 정규화 메뉴에서 스키마 목록을 불러오기 전에 다른 페이지로 이동할 경우 다시 정규화 메뉴로 돌아가는 문제 해결

스키마 목록이 많거나 네트워크 속도가 느린 환경에서 정규화 메뉴에 진입하여 스키마 목록을 불러오는 도중에 다른 페이지로 이동하면, 스키마 불러오기가 완료된 시점에 뒤늦게 다시 정규화 메뉴로 이동하는 문제를 해결했습니다.

#### SNR#1819 SNMP 트랩 수집기 삭제 후 동일 설정으로 다시 생성 시 실패하는 현상 해결

SNMP 트랩 수집기 삭제 후 이전과 동일한 설정으로 새 수집기를 생성한 경우, 수집기 삭제 작업 누락으로 인해 수집기 재생성 시 중복 오류가 발생하는 현상을 해결했습니다.

#### SNR#1921 소나 Angular SDK의 웹소켓 초기화 오류로 인해 앱이 반복적으로 웹소켓 접속을 시도하는 현상 해결

이전 버전의 소나 Angular SDK는 이미 암호화 키 협상이 완료된 웹소켓을 다시 협상하려고 시도하기 때문에 웹 브라우저의 자바스크립트 콘솔에 아래와 같은 오류가 발생합니다. 오류 발생 이후 다른 메뉴로 이동하면 접근 권한이 없다는 화면이 표시됩니다.

ERROR (websocket.service) no cipher\_suite matchedERROR TypeError: Cannot read properties of null (reading 'sigBytes')

새 버전의 소나 Angular SDK에서 이 문제를 해결하였습니다.