#### 시스로그

시스로그 수집기

시스템 설정 메뉴에서 지정한 시스로그 포트를 통해 실시간으로 TCP 및 UDP 시스로그를 수집하고 테이블에 저장할 수 있습니다.



* 원격지 IP: 원격지 IP를 입력합니다.
* 시스로그 설비 목록: PRI (<123> 같은 시스로그 헤더 부분)가 없는 경우 -1, 그렇지 않으면 쉼표 (,)로 facility 값을 이어붙여서 입력하면 됩니다. 가령 facility에 구분없이 해당 장비에서 발생하는 모든 시스로그를 수신하려고 한다면, RFC 5424에 나온대로 -1부터 23까지 모두 입력하면 됩니다. 아무 값도 입력하지 않으면 모든 facility을 입력한 것과 같습니다.
* 날짜 정규표현식: 시스로그에서 날짜 및 시각을 추출하는데 사용할 정규표현식을 입력합니다.
* 날짜 포맷: 정규표현식으로 추출한 날짜 데이터의 포맷을 입력합니다.
* 날짜 로케일: 날짜 문자열의 로케일. 가령 날짜 파싱 포맷의 지시자 중 MMM의 해석은 로케일에 따라 “Jan” 혹은 “1월”로 해석됩니다. 기본값은 en입니다.
* 시간대: 날짜 문자열의 시간대를 입력합니다. (예: KST 또는 Asia/Seoul)
* 정규식 필터: 추출할 데이터를 선별할 정규식 패턴을 입력합니다.
* 트랜스포머 설정: 수집된 로그에 적용할 트랜스포머를 선택합니다. "선택하세요."로 설정할 경우 트랜스포머가 적용되지 않고 원본 그대로 수집합니다. 트랜스포머에 대한 자세한 내용은 다음 항목을 참고하세요. 12.2.2 트랜스포머