#### 쿼리문 예시

다음 예시들을 통해 로그프레소 쿼리 문법의 구조, 명령어, 함수 및 사용법을 익힐 수 있습니다. 예제 테이블 syslog\_table과 ssh\_table을 대상으로 수행하는 쿼리문들입니다. 로그프레소 쿼리에 대해 더 자세히 알고 싶으시면 로그프레소 쿼리 설명서을 참고하시기 바랍니다.

예시 1

src\_zone 값이 Trust인 로그 최근 10000건 조회

table syslog\_table | parse ns | search src\_zone=="Trust" | limit 10000

예시 2

최근 1일 상위 10개 트래픽 src, dst 통계

table duration=1d syslog\_table | parse ns | stats count by src, dst | sort -count | limit 10 | eval seq=seq() | eval div=concat(seq, ". ", src, " -> ", dst)

예시 3

최근 7일간 일별 수집 건수 통계

table duration=7d syslog\_table | parse ns | eval day=string(\_time,"yyyy-MM-DD") | stats count by day

예시 4

최근 3일간 로그 중 rcvd가 sent보다 많은 로그 10000건 조회

table duration=3d syslog\_table | parse ns | search rcvd > sent | limit 10000

예시 5

최근 12시간동안 시간별 action Permit/Deny 건수 조회

table duration=12h syslog\_table | parse ns | eval hour=string(\_time,"yyyy-MM-DD HH:00:00") | stats count by hour, action | eval deny=if(action=="Deny",count,0), permit=if(action=="Permit",count,0) | stats sum(deny), sum(permit) by hour | rename sum(deny) as deny, sum(permit) as permit

예시 6

최근 1주일 SSH 로그인 성공/실패 건수 추출

table duration=7d ssh\_table | parse os | search in (result , "success","failure") | stats count by result

예시 7

최근 3일간 root계정 로그인 성공 회수 추출

table duration=3d ssh\_table | parse os | search account=="root" and type=="login" and result=="success" | stats count

예시 8

최근 3일간 result가 opened이거나 closed인 로그 추출

table duration=3d ssh\_table | parse os | search result=="opened" or result=="closed"

예시 9

최근 1개월간 일별로 로그인 실패가 가장 많이 발생한 IP 추출 (실패 회수가 같을 경우 해당 IP 모두 출력)

table duration=1mon ssh\_table | parse os | eval day=string(\_time,"yyyy-MM-DD") | search type=="login" and result=="failure" | stats count by day, src\_ip | stats max(count) by day | rename max(count) as count | join day, count [table duration=1mon ssh\_table | parse os | eval day=string(\_time,"yyyy-MM-DD") | search type=="login" and result=="failure" | stats count by day, src\_ip]

예시 10

가장 마지막 로그인 실패 내역 보기

table ssh\_table | parse os | search result=="failure" | sort -\_time | limit 1