### matchsig()

대상 표현식을 평가한 문자열에서 지정된 패턴 그룹 중 하나 이상의 패턴이 매칭되면 true, 매치되는 패턴이 없으면 false를 반환합니다.

#### 문법

matchsig(STR\_GUID, STR\_EXPR)

**STR\_GUID**

패턴 그룹 GUID. GUID 문자열은 유효한 패턴 그룹 식별자이어야 합니다. 유효하지 않은 패턴 그룹 GUID를 지정한 경우 쿼리가 실패합니다.

**STR\_EXPR**

검색 대상 문자열 표현식. 평가 값은 문자열이어야 합니다. 표현식을 평가할 수 없거나 유효하지 않은 값인 경우 false 를 반환합니다.

#### 설명

예를 들어, 아래 표와 같이 패턴 그룹에 패턴 "REMOTE\_ADDR" and ("fputs" or "fwrite") 검증식 path == "lib.php" 를 "zb now connect"라는 패턴 이름으로 설정한 경우, 대상 표현식 평가 값에서 REMOTE\_ADDR 문자열과 fputs 혹은 fwirte 문자열이 동시에 검색되는지 확인하고, 그 후에 path 필드 값이 lib.php 문자열과 일치하는지 확인합니다.

**패턴 예시**

|  |  |  |
| --- | --- | --- |
| expr (필수) | expr2 (선택) | rule (필수) |
| 키워드 패턴: 1차 고속 탐지 | 불린 표현식: 2차 필터링 | 패턴 이름 |
| "addextendedproc" and "xp\_cmdshell" |  | xp\_cmdshell |
| "REMOTE\_ADDR" and ("fputs" or "fwrite") | path == "lib.php" | zb now\_connect |