#### 위젯 실습용 데이터

실습용 테이블 만들기

위젯을 이해하는 가장 빠른 방법은 직접 만들어보는 것입니다. 위젯 실습에 사용하고자 GitHub 로그프레소 저장소에서 wp-nginx.log 파일을 가져와 로그프레소 플랫폼에 web\_example 테이블을 생성해서 사용합니다. 이 데이터는 2022년 4월 6일 오후 7시 35분부터 4월 7일 오전 0시 9분 사이에 워드프레스 서버에서 발생한 로그를 가져와 가공한 것입니다.

사용 중인 대시보드 프리셋이나 탭 패널을 변경하지 않도록 예제 실습용 프리셋이나 탭 패널을 따로 만들어서 위젯 예제를 따라해보시기 바랍니다.

쿼리문을 실행하는데 필요한 파서가 있는지 확인합니다.

* [파서를 적용해 데이터 추출하기](https://docs.logpresso.com/ko/enterprise/4.0/getting-started/query-drill)를 참고해서 apache\_log 파서가 있는지 확인하고, 없으면 만드십시오.
* 로그프레소 스토어에서 [아파치 웹 서버](https://logpresso.store/ko/apps/apache-httpd) 앱을 받아서 설치하고 앱이 제공하는 파서를 이용해도 됩니다.

다음 쿼리문을 실행해 예제에 필요한 데이터를 가져옵니다.

어느 쿼리문이든, 단 한 번만 실행하십시오. 여러번 실행하면 wedget\_example 테이블에 실행한 횟수만큼 중복된 데이터가 생깁니다. 여러 번 실행했다면 테이블을 삭제하고 다시 만드십시오.

# 아파치 웹 서버 앱이 설치되어 있지 않을 때 | wget url="https://raw.githubusercontent.com/logpresso/dataset/main/wp-nginx.log" | eval line = subarray(split(line, "\n"), 0) | explode line | parse apache\_log | split field=request sep=" " overlay=t method, uri, version | split field=uri field=uri sep="?" overlay=t path, query | rename date as \_time, remote\_host as src\_ip, resp\_bytes\_clf as sc\_bytes | lookup geoip src\_ip output country, asn | fields \_time, src\_ip, country, asn, status, method, path, query, version, sc\_bytes, user\_agent, referer | import create=t widget\_example

# 아파치 웹 서버 앱이 설치되어 있을 때 | wget url="https://raw.githubusercontent.com/logpresso/dataset/main/wp-nginx.log" | eval line = subarray(split(line, "\n"), 0) | explode line | parse apache\_httpd\_combined\_norm | import create=t widget\_example

데이터소스 만들기

데이터소스는 데이터 위젯을 구성할 때 호출해 사용하는 데이터 쿼리문을 의미합니다. 데이터소스는 위젯을 구성하는 단계에서 추가, 수정, 삭제할 수 있습니다. 자세한 내용은 [대시보드 만들기](https://docs.logpresso.com/ko/enterprise/4.0/ui/dashboard-tutorial)에서 [데이터소스](https://docs.logpresso.com/ko/enterprise/4.0/ui/dashboard-tutorial)를 참고하십시오.

데이터 위젯에서 다루는 예제를 실습하려면 다음 쿼리문을 데이터소스 목록에 widget\_example으로 등록하여 사용하시기 바랍니다.

set from=nvl($("from"), dateadd(now(), "year", -5))| set to=nvl($("to"), string(now(), "yyyyMMddHHmmss"))| set site="https://example.com"| table from=$("from") to=$("to") widget\_example| eval suspicious = case( path == "\*/../\*" or path == "\*/./\*", "dir\_traversal", path == "/.\*", "dotfile\_access", path == "/temp\*" or path == "/tmp\*", "temp\_file\_access", path == "/bbs/login\*", "login\_access", path == "\\\*", "path\_anomaly", path == "\\*", "wildcard", method == "POST", "post", method == "PRI", "pri", method == "CONNECT", "connect", method == "GET" or method == "OPTIONS" or method == "HEAD", "normal", "method\_anomaly" ), url = if(isnull(query), concat(site, path), concat(site, path, "?", query))| search case( isnull($("type")), true, typeof($("type"))=="string", suspicious==($("type")), typeof($("type"))=="object[]", -1 != indexof(string($("type")), suspicious), false ) and if(isnull($("method")),true,contains(method,$("method")))

widget\_example으로 등록한 데이터소스에서 from, to, type, method는 모두 [쿼리 매개변수](https://docs.logpresso.com/ko/query/query-syntax)로 사용할 수 있습니다. 쿼리 매개변수의 사용은 [컨트롤 위젯](https://docs.logpresso.com/ko/enterprise/4.0/ui/control-widgets)에서 다룹니다.

* from, to를 제어하는 예시는 [날짜 컨트롤](https://docs.logpresso.com/ko/enterprise/4.0/ui/control-widget-date-picker)에서 확인할 수 있습니다.
* type를 제어하는 예시는 [다중 선택 컨트롤](https://docs.logpresso.com/ko/enterprise/4.0/ui/control-widget-check-box), [리스트 컨트롤](https://docs.logpresso.com/ko/enterprise/4.0/ui/control-widget-select-box)에서 확인할 수 있습니다.
* method를 제어하는 예시는 [텍스트 컨트롤](https://docs.logpresso.com/ko/enterprise/4.0/ui/control-widget-text-input)에서 확인할 수 있습니다.