### table

로그프레소 테이블에 저장된 데이터를 조회합니다. 관리자는 모든 테이블을, 사용자는 자신에게 읽기 권한이 부여된 테이블만 조회할 수 있습니다.

#### 문법

지정한 기간만큼 최근에 저장된 데이터를 조회

table duration=INT{mon|w|d|h|m|s} [limit=INT] [offset=INT] [order=STR] NODE:TABLE, [...]

from, to 옵션 중 하나만 지정하거나, 모두 지정하여 특정 기간에 속하는 데이터만 조회

table [from=yyyyMMddHHmmss] [to=yyyyMMddHHmmss] [limit=INT] [offset=INT] [order=STR] NODE:TABLE, [...]

쿼리 실행 시점부터 지정된 기간만큼 테이블에 기록되는 데이터를 조회

table window=INT{y|mon|w|d|h|m|s} [limit=INT] [offset=INT] [order=STR] NODE:TABLE, [...]

**duration=INT{mon|w|d|h|m|s}**

지정한 시간만큼 최근 데이터만 검색. mon(월), w(주), d(일), h(시), m(분), s(초) 단위와 함께 입력하세요. 10s은 쿼리 실행 시각을 기준으로 "최근 10초"를 의미합니다. 이 옵션은 from, to, window와 함께 사용할 수 없습니다.

**from=yyyyMMddHHmmss**

검색할 기간의 시작 시각을 yyyyMMddHHmmss 형식으로 지정. 입력한 시각부터 검색을 시작합니다. 앞부분만 입력하면 나머지 자리는 0으로 인식합니다. 예를 들어 20130605를 입력하면 20130605000000 (2013년 6월 5일 0시 0분 0초)으로 인식합니다. 이 옵션은 to와 함께 사용할 수 있지만, duration, window는 함께 사용할 수 없습니다.

**to=yyyyMMddHHmmss**

검색할 기간의 끝 시각을 yyyyMMddHHmmss 형식으로 지정. 입력한 시각은 검색 범위에 포함되지 않습니다. 입력 방식은 from과 같습니다. from과 함께 사용할 수 있지만, duration, window는 함께 사용할 수 없습니다.

**window=INT{y|mon|w|d|h|m|s}**

쿼리 실행 시점부터 어느 정도의 시간 동안 테이블에 입력되는 데이터를 실시간으로 수신할 것인지 지정. y(연), mon(월), w(주), d(일), h(시), m(분), s(초) 단위와 함께 입력하세요. 단위가 y일 때, 1y만 허용됩니다. 10s은 쿼리 실행 시각을 기준으로 “앞으로 10초”입니다. 이 옵션은 duration, from, to와 함께 사용할 수 없습니다.

duration, from, to, window 옵션 중 하나라도 지정하지 않으면 테이블에 지정된 모든 데이터를 조회합니다. 가급적 조회 대상 기간을 지정하세요.

**limit=INT**

가져올 최대 로그 개수(기본값: 제한 없음)

**offset=INT**

건너뛸 로그 개수(기본값: 0).

**order=STR**

레코드의 정렬 순서 (기본값: desc)

1. asc: 오름차순 정렬. 오래된 레코드부터 출력.
2. desc: 내림차순 정렬. 최근 레코드부터 출력.

**NODE:TABLE, [...]**

검색할 테이블 경로. NODE:TABLE을 여러 개 지정하려면 쉼표(,)를 구분자로 사용하세요. 와일드카드(\*)를 사용할 수 있습니다.

**NODE**

([클러스터](https://docs.logpresso.comnull) 환경에서) 노드 페어의 이름 또는 노드 ID. 테이블을 생성하면 모든 노드에 동일한 이름으로 테이블이 생성되므로 로그프레소 쿼리로 테이블에 저장된 데이터에 접근하려면 테이블 경로를 함께 명시해야 합니다.

1. 노드의 로컬 테이블을 조회할 때, 테이블 경로(NODE)를 생략할 수 있습니다.
2. 클러스터 구성일 때, [수집기](https://docs.logpresso.comnull)의 **적재 위치** 설정에 따라
3. **적재 위치**가 **부하 균등 분배**일 때, 데이터는 모든 노드의 테이블에 분산되어 저장되므로 **NODE**에 와일드카드(\*)를 지정하세요.
4. **적재 위치**가 **노드 페어**일 때, 수집된 데이터는 특정 노드 페어의 테이블에 저장되므로 **NODE**에 **노드 페어 이름** 또는 **노드 ID**를 지정하세요.

**콜론(:)**

노드 페어의 이름 또는 노드 ID와 테이블 구분자. 콜론 전후로 공백문자가 없게 주의하세요.

**TABLE**

조회할 테이블 이름. 와일드카드(\*)를 사용할 수 있습니다.

1. 이름 뒤에 물음표(?)를 붙이면 해당 테이블이 존재하지 않아도 오류가 발생하지 않습니다. 가령, sys\_status 테이블이 존재하지 않을때 table sys\_status 쿼리를 실행하면 오류가 발생하지만, table sys\_status? 쿼리를 실행하면 오류 없이 쿼리가 수행되며 결과 0건이 출력됩니다.
2. 이름의 시작이나 끝에 와일드카드(\*)를 사용할 수 있습니다. 예를 들어, 쿼리문 table sys\_\*를 실행하면 sys\_로 시작하는 테이블들 중에서 읽기 권한이 없는 테이블을 제외하고 모두 조회합니다. 쿼리를 실행한 다음 **\_table** 필드에서 테이블 이름을 확인할 수 있습니다.

#### 설명

출력 필드

이 명령어는 조회할 데이터의 모든 필드를 출력합니다. 그 외에 모든 테이블은 다음과 같은 메타데이터 필드를 포함할 수 있습니다.

|  |  |  |  |
| --- | --- | --- | --- |
| 필드 | 타입 | 이름 | 설명 |
| \_table | 문자열 | 테이블 | 레코드가 저장된 테이블 이름 |
| \_time | 날짜 | 시각 | 레코드 기록 일시 |
| \_era | 64비트 정수 | 파티션 식별자 | 스토리지 계층화를 지원하지 않는 파티션은 0으로 표시 |
| \_id | 64비트 정수 | 번호 | 파티션 내에서 유일한 레코드의 일련번호 |
| \_device\_ip | IP 주소 | 원천 IP | 데이터 원천 호스트의 IP 주소 |
| \_device\_name | 문자열 | 원천 호스트 | 데이터 원천 호스트의 이름 |
| \_file | 문자열 | 파일 이름 | 원본 데이터 파일 이름 |
| \_logger | 32비트 정수 | 수집기 번호 | 수집기의 일련번호 |
| \_logger\_name | 문자열 | 수집기 이름 | 접두사 sonar\_logger\_와 수집기 번호의 조합 |
| \_node | 문자열 | 노드 ID |  |
| \_schema | 문자열 | 로그 스키마 식별자 | 정규화에 적용된 로그 스키마의 식별자(예: auth) |
| \_site | 문자열 | 사이트 |  |
| line | 문자열 | 원본 | 데이터 원본을 문자열로 표현한 값 |

#### 사용 예

sys\_cpu\_logs 테이블에서 최근 기록된 100건의 데이터 조회

# 로컬 노드 sys\_cpu\_logs 테이블 조회 | table limit=100 sys\_cpu\_logs

# 모든 노드의 sys\_cpu\_logs 테이블 조회 | table limit=100 \*:sys\_cpu\_logs

sys\_cpu\_logs 테이블에서 최근 10분 간 기록된 데이터 조회

# 로컬 노드의 sys\_cpu\_logs 테이블 조회 table duration=10m \*:sys\_cpu\_logs

# 모든 노드의 sys\_cpu\_logs 테이블 조회 table duration=10m \*:sys\_cpu\_logs

모든 노드의 sys\_cpu\_logs 테이블에서 2013년 6월 5일에 기록된 데이터 조회

table from=20130605 to=20130606 \*:sys\_cpu\_logs

모든 노드에서 sys\_cpu\_logs 테이블과 sys\_mem\_logs 테이블에 기록된 모든 데이터를 오래된 것부터 조회

table order=asc \*:sys\_cpu\_logs, \*:sys\_mem\_logs