### table

ログプレッソ・ソナーのテーブルに保存されたデータを検索します。管理者はすべてのテーブルを、ユーザーは自身に読み取り権限が付与されたテーブルのみを検索できます。

#### 構文

指定した期間分、直近に保存されたデータを検索

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

from、toオプションのいずれか、または両方を指定して、特定期間に該当するデータのみを検索

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

クエリ実行時点から指定した期間分、テーブルに記録されるデータを検索

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}**

指定した時間分、直近のデータのみを検索します。mon（月）、w（週）、d（日）、h（時）、m（分）、s（秒）単位で入力してください。たとえば10sはクエリ実行時点を基準に「直近10秒」を意味します。このオプションはfrom、to、windowと同時に使用できません。

**from=yyyyMMddHHmmss**

検索期間の開始時刻をyyyyMMddHHmmss形式で指定します。入力した時刻から検索を開始します。先頭部分のみ入力した場合、残りの桁は0として認識されます。例：20130605と入力すると20130605000000（2013年6月5日0時0分0秒）として認識されます。このオプションはtoと併用できますが、duration、windowとは併用できません。

**to=yyyyMMddHHmmss**

検索期間の終了時刻をyyyyMMddHHmmss形式で指定します。入力した時刻は検索範囲に含まれません。入力方法はfromと同様です。fromと併用できますが、duration、windowとは併用できません。

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

クエリ実行時点から指定した期間、テーブルに入力されるデータをリアルタイムで受信します。y（年）、mon（月）、w（週）、d（日）、h（時）、m（分）、s（秒）単位で入力してください。単位がyの場合は1yのみ指定可能です。10sはクエリ実行時点を基準に「今後10秒間」を意味します。このオプションはduration、from、toと同時に使用できません。

duration、from、to、windowオプションのいずれも指定しない場合、テーブル内のすべてのデータを検索します。できるだけ検索対象期間を指定してください。

**limit=INT**

取得する最大ログ件数（デフォルト：制限なし）

**offset=INT**

スキップするログ件数（デフォルト：0）

**order=STR**

レコードのソート順（デフォルト：desc）

1. asc: 昇順ソート。古いレコードから出力。
2. desc: 降順ソート。新しいレコードから出力。

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

検索対象のテーブルパス。複数指定する場合はカンマ（,）で区切ります。ワイルドカード（\*）が使用可能です。

**NODE**

（[クラスター](https://docs.logpresso.comnull)環境の場合）ノードペア名またはノードID。テーブルを作成するとすべてのノードに同じ名前でテーブルが作成されるため、ログプレッソ・ソナーのクエリでテーブルデータにアクセスするにはテーブルパスを明示する必要があります。

1. ノードのローカルテーブルを検索する場合、テーブルパス（NODE）は省略可能です。
2. クラスター構成の場合、[ロガー](https://docs.logpresso.comnull)の**格納先**設定により
3. **格納先**が**負荷分散**の場合、データはすべてのノードのテーブルに分散保存されるため、**NODE**にワイルドカード（\*）を指定してください。
4. **格納先**が**ノードペア**の場合、収集データは特定ノードペアのテーブルに保存されるため、**NODE**に**ノードペア名**または**ノードID**を指定してください。

**コロン(:)**

ノードペア名またはノードIDとテーブルの区切り文字。コロン前後に空白を入れないようご注意ください。

**TABLE**

検索対象のテーブル名。ワイルドカード（\*）が使用可能です。

1. 名前の末尾にクエスチョンマーク（?）を付けると、該当テーブルが存在しなくてもエラーになりません。例えば、sys\_statusテーブルが存在しない場合、table sys\_statusクエリを実行するとエラーになりますが、table sys\_status?クエリを実行するとエラーなくクエリが実行され、結果は0件となります。
2. 名前の先頭または末尾にワイルドカード（\*）を使用できます。例えば、クエリtable sys\_\*を実行すると、sys\_で始まるテーブルのうち、読み取り権限があるものすべてを検索します。クエリ実行後、**\_table**フィールドでテーブル名を確認できます。

#### 説明

出力フィールド

このコマンドは、検索対象データのすべてのフィールドを出力します。加えて、すべてのテーブルには以下のようなメタデータフィールドが含まれる場合があります。

|  |  |  |  |
| --- | --- | --- | --- |
| フィールド | 型 | 日本語名 | 説明 |
| \_table | 文字列 | テーブル | レコードが保存されたテーブル名 |
| \_time | 日付 | 時刻 | レコード記録日時 |
| \_era | 64ビット整数 | パーティションID | ストレージ階層化非対応パーティションは0で表示 |
| \_id | 64ビット整数 | 番号 | パーティション内で一意なレコードのシリアル番号 |
| \_device\_ip | IPアドレス | 元IP | データ元ホストのIPアドレス |
| \_device\_name | 文字列 | 元ホスト | データ元ホスト名 |
| \_file | 文字列 | ファイル名 | 元データファイル名 |
| \_logger | 32ビット整数 | ロガー番号 | ロガーのシリアル番号 |
| \_logger\_name | 文字列 | ロガー名 | プレフィックスsonar\_logger\_＋ロガー番号 |
| \_node | 文字列 | ノードID |  |
| \_schema | 文字列 | ログスキーマID | 正規化に適用されたログスキーマID（例：auth） |
| \_site | 文字列 | サイト |  |
| line | 文字列 | 元データ | データ元を文字列で表現した値 |

#### 使用例

sys\_cpu\_logsテーブルから直近100件のデータを検索

# ローカルノードのsys\_cpu\_logsテーブルを検索 | table limit=100 sys\_cpu\_logs

# すべてのノードのsys\_cpu\_logsテーブルを検索 | table limit=100 \*:sys\_cpu\_logs

sys\_cpu\_logsテーブルから直近10分間に記録されたデータを検索

# ローカルノードのsys\_cpu\_logsテーブルを検索 table duration=10m \*:sys\_cpu\_logs

# すべてのノードのsys\_cpu\_logsテーブルを検索 table duration=10m \*:sys\_cpu\_logs

すべてのノードのsys\_cpu\_logsテーブルから2013年6月5日に記録されたデータを検索

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

すべてのノードでsys\_cpu\_logsテーブルとsys\_mem\_logsテーブルに記録された全データを古い順で検索

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