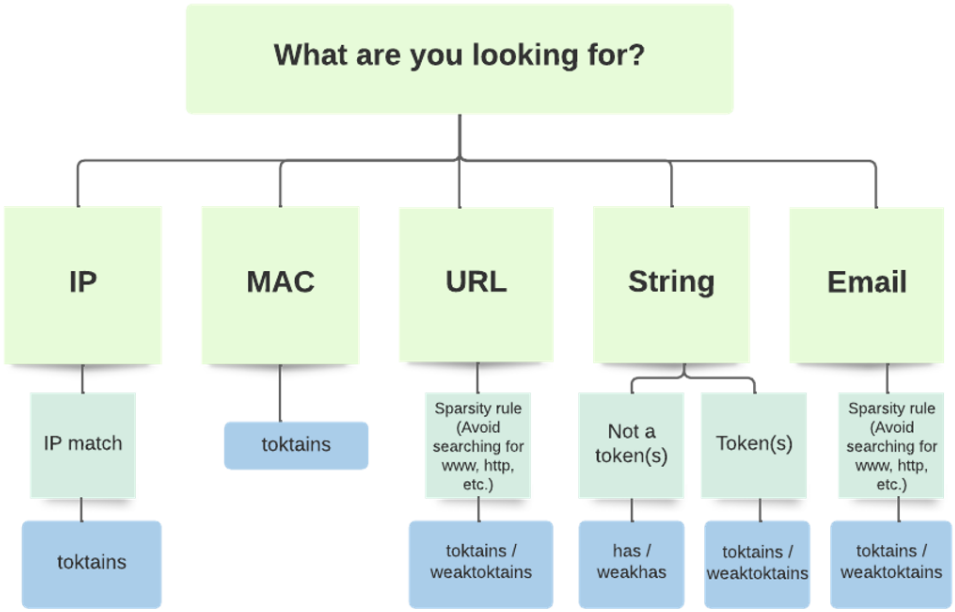
Choosing the Right Operation for your Query

1 month ago • 0 replies



yul pertierra

Choosing the right operation for your query can be challenging. The purpose of this article is to give you a better understanding of how different use cases relate to Devo operations.

This article contains key information about each of the operations mentioned, including how to apply them and query examples, as well as a visual resource you can download and use in your day-to-day work.

Operations

Toktains

> This operation is **case-sensitive.**
>
> Check *weaktoktains* section for case-insensitive *toktains*.

Overview

Tokenization is used by Devo to index values in raw data**. A token is simply a string of alphanumeric characters separated by ASCII symbols** (non-alphanumeric characters like symbols and spaces) in the raw event as it was delivered to Devo.

Here's an example:

- value: `user.company@devo.com`
  - tokens: `.` `@`
  - tokenized-items: `user` `company` `devo` `com`

How it works

You can apply this operation either as a **Filter** or **Create column** operation:

- **Filter**. Creates a filter that returns only those strings including a specific token. Optionally, you can add one or two boolean values to extend the left and right length of the token.

Example:

```
from demo.ecommerce.data
where toktains(uri, "09", true, false)
```

- **Create column.** Adds a new Boolean column that shows true when a specific token is present in a given string. Optionally, you can add one or two boolean values to extend the left and right length of the token.

Example:

```
from demo.ecommerce.data
select toktains(uri, "09", true, false) as token_09
```

In addition, leveraging the `toktains(raw, "value")` operation is the quickest way to leverage the index in Devo, reducing the total amount of data read and leading to optimal experience while querying in Devo.

Learn more about working with toktains.

> Notice that if you are searching for an URL or email you should apply the **sparsity law** (avoid searching for www, http, .com, etc.)

Weaktoktains

Overview

Case-insensitive *toktains*.

How it works

You can apply this operation either as a **Filter** or **Create column** operation:

- **Filter**. Creates a filter that returns only those strings including a specific token, ignoring case. Optionally, you can add one or two boolean values to extend the left and right length of the token.

Example:

```
from siem.logtrust.web.activity
where weaktoktains(headers, "language")
```

- **Create column.** Adds a new Boolean column that shows true when a specific token is present in a given string, ignoring the case. Optionally, you can add one or two boolean values to extend the left and right length of the token.

Example:

```
from siem.logtrust.web.activity
select weaktoktains(headers, "language") as token_language
```

Learn more about weaktoktains.

Has

> This operation is **case-sensitive.**
>
> Check *weakhas* section for case-insensitive *has*.

Overview

Has is *a string-group operation.* Use it to check the presence of a value or a group of values within a specific string.

How it works

You can apply this operation either as a **Filter** or **Create column** operation:

- **Filter**. Checks for the presence of one or more values in a given string. The filter will identify those strings containing at least one of the indicated values.

Example:

```
from demo.ecommerce.data
where has(timestamp, "24", "25")
```

- **Create column.** Creates a Boolean column that shows true when at least one of the indicated values is present in the given string.

Example:

```
from demo.ecommerce.data
select has(timestamp, "24", "25") as has_24_or_25
```

Learn more about has.

Weakhas

Overview

Case-insensitive *has*.

How it works

You can apply this operation either as a **Filter** or **Create column** operation:

- **Filter**. Returns only those strings that contain a specified value, ignoring case.

Example:

```
from demo.ecommerce.data
where weakhas(userAgent, "mozilla")
```

- **Create column.** Creates a Boolean column that shows true when the indicated value is present in the given string, ignoring case.

Example:

```
from demo.ecommerce.data
select weakhas(userAgent, "mozilla") as has_mozilla_ins
```

Learn more about *weakhas.*

How To | LINQ | Querying | Data search

 2 people like this

Did this topic help you find an answer to your question?

0 replies

Be the first to reply!