

Demonstrates how to use Sumo Logic query language

gist.github.com/Integralist/8236c15562389b10b576

262588213843476



Demonstrates how to use Sumo Logic query language

Take log message and parse as JSON (create new column `jsonobj`):

```
parse "*" as jsonobj
```

Take new `jsonobj` column and create a new column for the specified key in the JSON:

```
json field=jsonobj "my-obj-key"
```

Allow extracting multiple keys from the json object:

```
json field=jsonobj "event", "url" as event, url
```

Extract a regex match:

```
parse regex field=url "cps/asset/(?<asset_id>[^\?]+)"
```

Requires the use of a named capturing group
(?

Indicate case insensitivity with **(?i)**:

```
(?<a_match>(i)topics)
```

Parse contents out from the default **message** column:

```
_collector=Mozart | where component="mozart-routing" | where  
environment="int" | parse "HTTPD*" as Apache
```

You can use a different format as well:

```
(_collector=Mozart) environment = "live" component = "mozart-composition"
```

```
_collector=Newsbeat AND read_feed | where environment = "live" | where component =  
"newsbeat-most-popular-renderer"
```

```
_collector=Mozart | where component="mozart-composition" | where environment="int" |  
parse "*" as jsonobj | json field=jsonobj "event" | where event="ComponentLoaded"
```

```
_collector= Newsbeat | parse "*" as jsonobj | json field=jsonobj "event", "url" as event, url  
| where component="newsbeat-article-renderer" | parse regex field=url "cps/asset/(?  
<asset_id>[^\?]+)"
```

```
_collector= Newsbeat | parse "*" as jsonobj | json field=jsonobj "event", "url" as event, url  
| where component="newsbeat-article-renderer" | parse regex field=event "(?<a_match>  
(i)topics)"
```

Leave a comment

[Markdown is supported](#) |