Splunk Queries

Count Events per Index

```
| tstats count WHERE index=* OR index=_* by index
```

List Indexes

```
| eventcount summarize=false index=* | dedup index | fields index
```

Events per Host / Index / Sourcetype

```
| tstats count as EVENTS_PER_HOST where index=* by index,sourcetype,host |
table * | sort by index
```

kb, splunk

From:
http://fortytwo.adurias.org/ - **Fortytwo - Answer to the Ultimate Question of Life, the Universe, and Everything**

Permanent link:
http://fortytwo.adurias.org/splunk-queries?rev=1706170621

Last update: **2024/01/25 09:17**