

# Splunk Queries

## Indexes & Events

### List Indexes

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

### Count Events per Index

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

```
| tstats count where index=<indexname> by _time host span=1h prestats=true
| timechart count span=1h
| addtotals
```

### Events per Host / Index / Sourcetype

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

### Ingestion by Index

```
index=_internal sourcetype=splunkd source=*license_usage.log type=Usage
| stats sum(b) as bytes by idx | eval mb=round(bytes/1024/1024,3)
```

### Timechart

```
index=_internal sourcetype=splunkd source=*license_usage.log type=Usage
| timechart span=1d sum(b) as usage by idx limit=0
| foreach * [ eval "<<FIELD>>"=round('<<FIELD>>'/1024/1024,3)]
```

### Total Ingestion

```
index=_internal sourcetype=splunkd source=*license_usage.log type=Usage
| timechart span=1d sum(b) as usage
| eval gb=round(usage/1073741824,3)
```

```
| table _time, gb
```

## Lookups & Macros

### Export Lookup file

```
| inputlookup my_lookup.csv
```

### List of Macros

```
| rest /servicesNS/-/-/admin/macros count=0
```

[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>

Last update: **2024/10/15 05:26**

