Splunk Queries

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 cound 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)]
```

Export Lookup file

```
| inputlookup my_lookup.csv
```

List of Macros

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

kb, splunk