

Splunk total run time

```
(index=_audit host=* action=search sourcetype=audittrail search_id!="rsa_*")
| eval user = if(user="n/a", null(), user)
| eval search_id=replace(search_id, "'(.*)'", "\1")
| eval search=if(isnull(savedsearch_name) OR savedsearch_name="", search, savedsearch_name)
| stats min(_time) as _time, values(user) as user, max(total_run_time) as total_run_time,
first(search) as search, first(apiStartTime) as apiStartTime, first(apiEndTime) as apiEndTime
by search_id
```

Revision #1

Created 23 March 2022 16:03:29 by Clinton

Updated 23 March 2022 16:03:51 by Clinton