
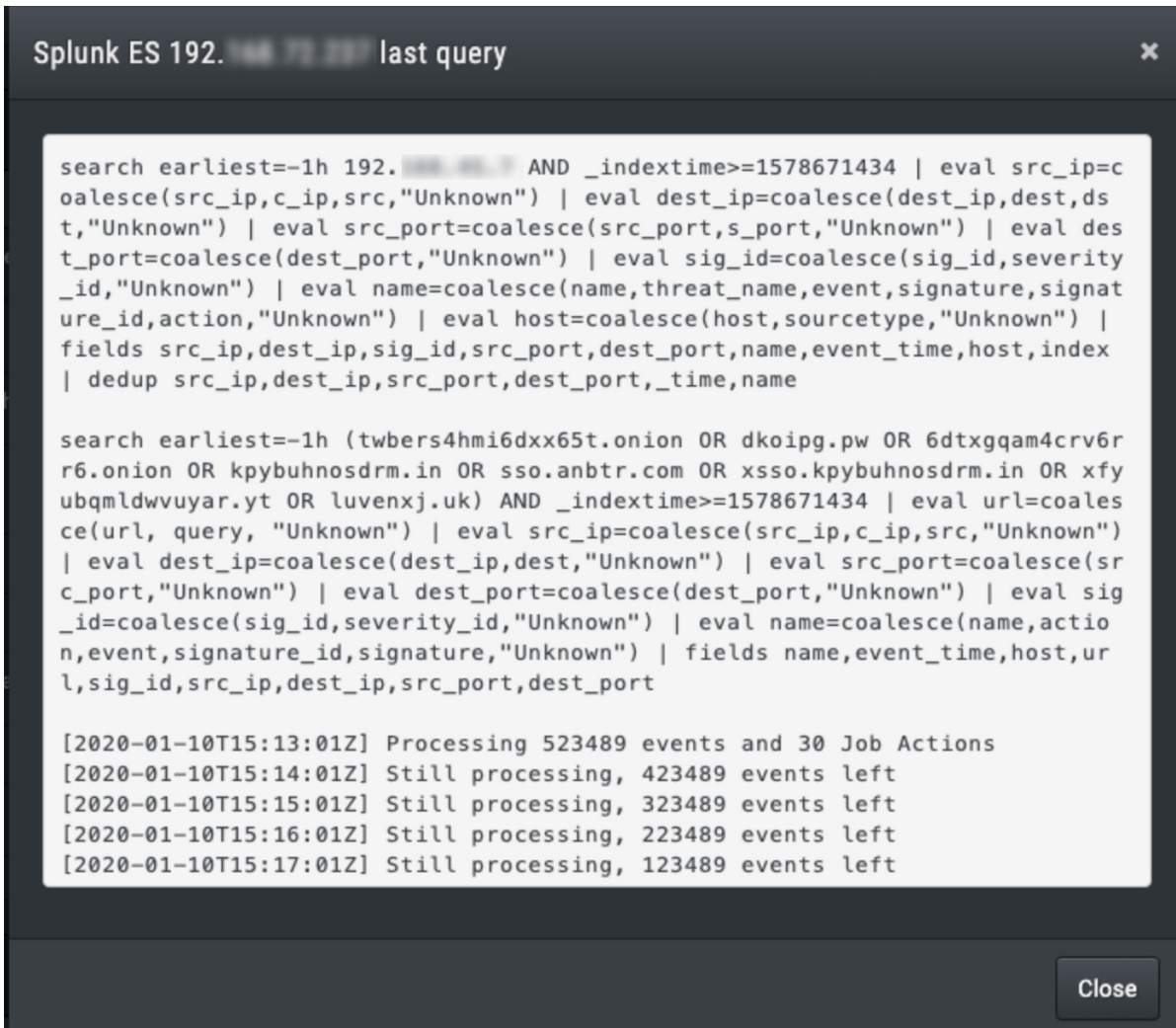


JOB IS MISSING EVENTS - SPLUNK / SPLUNK ES

When a Job causes a high number of events, it can appear that the integration stops processing subsequent Jobs when in fact the events are still being processed. To determine if this is the case, go to **Settings > Integrations** and click **View Last Query**  for the integration. If events are still processing, you'll see processing messages, as displayed in the Splunk last query image.



```
Splunk ES 192.168.72.200 last query X

search earliest=-1h 192.168.72.200 AND _indextime>=1578671434 | eval src_ip=coalesce(src_ip,c_ip,src,"Unknown") | eval dest_ip=coalesce(dest_ip,dest,dest,"Unknown") | eval src_port=coalesce(src_port,s_port,"Unknown") | eval dest_port=coalesce(dest_port,"Unknown") | eval sig_id=coalesce(sig_id,severity_id,"Unknown") | eval name=coalesce(name,threat_name,event,signature,signature_id,action,"Unknown") | eval host=coalesce(host,sourcetype,"Unknown") | fields src_ip,dest_ip,sig_id,src_port,dest_port,name,event_time,host,index | dedup src_ip,dest_ip,src_port,dest_port,_time,name

search earliest=-1h (twbers4hmi6dxx65t.onion OR dkoipg.pw OR 6dtxgqam4crv6r6.onion OR kpybuhnosdrm.in OR sso.anbtr.com OR xssso.kpybuhnosdrm.in OR xfyubqmlwvuyar.yt OR luvenxj.uk) AND _indextime>=1578671434 | eval url=coalesce(url,query,"Unknown") | eval src_ip=coalesce(src_ip,c_ip,src,"Unknown") | eval dest_ip=coalesce(dest_ip,dest,"Unknown") | eval src_port=coalesce(src_port,"Unknown") | eval dest_port=coalesce(dest_port,"Unknown") | eval sig_id=coalesce(sig_id,severity_id,"Unknown") | eval name=coalesce(name,action,event,signature_id,signature,"Unknown") | fields name,event_time,host,url,sig_id,src_ip,dest_ip,src_port,dest_port

[2020-01-10T15:13:01Z] Processing 523489 events and 30 Job Actions
[2020-01-10T15:14:01Z] Still processing, 423489 events left
[2020-01-10T15:15:01Z] Still processing, 323489 events left
[2020-01-10T15:16:01Z] Still processing, 223489 events left
[2020-01-10T15:17:01Z] Still processing, 123489 events left

Close
```

Splunk ES last query showing events still in process