The heap memory profile of splunkd can be collected

The configuration options include:

prof: true

prof\_accum: true

prof\_leak: true

lg\_prof\_interval: 36 (see box below)

prof\_prefix: <directory for heap data>

Enable Heap Dump

1)Create a temporary directory to collect the data.

mkdir -p /tmp/

2)Add these settings to splunk-launch.conf:

LD\_PRELOAD=/opt/splunk/lib/with\_stats/libjemalloc.so

MALLOC\_CONF="prof:true,prof\_accum:true,prof\_leak:true,lg\_prof\_interval:32,prof\_prefix:/opt/splunk/tmp/heap\_data"

NOTE :

lg\_prof\_interval

The data will be dumped in intervals determined by the parameter lg\_prof\_interval, which is the log base 2 of the total allocation between two dumps. With a value of 30, it will dump every 1GB of allocation, and with a value of 36, it will dump every 64GB of allocation. Note that it is the total allocation between dumps, not the live allocations at that time. A value of 36 should work fine for most scenarios to avoid filling up disk space too soon. Typical memory on splunk EC2 search heads is around 140GB. If the issue causes a slower memory growth, say over days, consider using a higher value for lg\_prof\_interval. You can also use a lower value if the memory spike is too rapid.

3)After starting Splunk, heap data will start collecting in the directory specified in the prof\_prefix option.

4)Stop Splunk at any time to stop collecting heap data.