Elasticsearch Monitoring

Why doesn't the number of documents I see in SPM match the number of documents in my Elasticsearch index

SPM collects index stats from primary shards only. To see the total number of documents in an index, select all shards in that index and choose "sum". The list of shards and the "sum" function can be found in the "Shard filter" in the Index Stats report.

Can SPM collect metrics even when Elasticsearch HTTP API is disabled

Each SPM agent collects Elasticsearch metrics only from the local node by accessing the Stats API via HTTP. To allow only local access add the following to elasticsearch.yml. Don't forget to restart each ES node to whose elasticsearch.yml you add this.

```
http.host: "127.0.0.1"
```

Can I point SPM monitor to a non-localhost Elasticsearch node

Yes. Adjust /opt/spm/spm-monitor/conf/spm-monitor-config-*TOKEN_HERE*-default.properties and change the SPM_MONITOR_ES_NODE_HOSTPORT property from the default localhost:9200 value to use an alternative hostname:port. After that restart SPM monitor (if you are running a standalone version) or Elasticsearch process(es) with embedded SPM monitor.

My Elasticsearch is protected by basic HTTP authentication, can I use SPM

Yes. You just need to adjust /opt/spm/spm-monitor/conf/spm-monitor-config-*TOKEN_HERE*-default.properties file by adding the following two properties (replace values with your real username and password):

```
SPM_MONITOR_ES_NODE_BASICAUTH_USERNAME=yourUsername
SPM_MONITOR_ES_NODE_BASICAUTH_PASSWORD=yourPassword
```

Restart your SPM monitor after this change (either with **sudo service spm-monitor restart** in case of standalone monitor or by restarting Elasticsearch node if you are using in-process javaagent).

I am using SPM for Elasticsearch monitor and I don't see Index (and/or Refresh/Flush/Merge) stats, why is that

SPM for Elasticsearch monitor collects Index stats only from primary shards, so it is possible that you installed SPM monitor on some Elasticsearch node which hosts only replicas. The same is also true for Refresh/Flush and Merge stats. Also note that SPM Elasticsearch monitor should be installed on all your Elasticsearch nodes to get the complete picture of your cluster in SPM Reports UI.

Integration

- Instructions: https://apps.sematext.com/ui/howto/Elasticsearch/overview

Metrics

Metric Name	Key	Agg	Type	Description
overhead	es.circuitBreaker.fieldData.overhead	Avg	Double	
maximum size	es.circuitBreaker.fieldData.max	Max	Long	
estimated size	es.circuitBreaker.request.estimate	Avg	Long	
estimated size	es.circuitBreaker.fieldData.estimate	Avg	Long	
overhead	es.circuitBreaker.request.overhead	Avg	Double	
maximum size	es.circuitBreaker.request.max	Max	Long	
initializing shards	es.cluster.health.shards.initializing	Avg	Long	
relocating shards	es.cluster.health.shards.relocating	Avg	Long	
nodes	es.cluster.nodes	Avg	Long	

Metric Name	Key	Agg	Type	Description
data nodes	es.cluster.data_nodes	Avg	Long	
active primary shards	es.cluster.health.active_primary_shards	Avg	Long	
unassigned shards	es.cluster.health.unassigned_shards	Avg	Long	
active shards	es.cluster.health.active_shards	Avg	Long	
filter cache size	es.cache.filter.size	Avg	Long	max
field cache evictions	es.cache.field.evictions	Sum	Long	
current	es.cache.warmer.current	Avg	Long	
filter cache evictions	es.cache.filter.evictions	Sum	Long	
total	es.cache.warmer.total	Sum	Long	
filter cache count	es.cache.filter.count	Avg	Long	
total time	es.cache.warmer.time	Sum	Long	

Metric Name	Key	Agg	Type	Description
field cache size	es.cache.field.size	Avg	Long	
open HTTP conns (current_open)	es.connection.http.current.open	Avg	Long	
socket resets sent (out_rsts)	es.connection.out.rsts	Sum	Long	
received count (rx_count)	es.transport.rx.packets	Sum	Long	
passive conn openings (passive_opens)	es.connection.passive.opens	Sum	Long	
outbound segments (out_segs)	es.connection.out.segs	Sum	Long	
received size (rx_size)	es.transport.rx.bytes	Sum	Long	
open TCP conns (server_open)	es.connection.server.open	Avg	Long	

Metric Name	Key	Agg	Type	Description
transmitted transport size (tx_size)	es.transport.tx.bytes	Sum	Long	Total bytes
failed socket open (attempt_fails)	es.connections.tcp.attempt.fails	Sum	Long	Total failed socket open attempts
socket resets (estab_resets)	es.connections.tcp.estab.resets	Sum	Long	Total socket resets
total opened HTTP conns (total_opened)	es.connections.total.opened	Avg	Long	Total opened HTTP conns
inbound segments (in_segs)	es.connections.tcp.in.segs	Sum	Long	Total inbound segments
open sockets (current_estab)	es.connections.tcp.current.estab	Avg	Long	Total open sockets
active conn openings (active_opens)	es.connections.tcp.avtive.opens	Sum	Long	Total active conn openings

Metric Name	Key	Agg	Type	Description
retransmitted segments (retrans_segs)	es.tcp.retrans	Sum	Long	Total retrans.segs
transmitted count (tx_count)	es.transport.tx.count	Sum	Long	Total packets
queue	es.thread_pool.queue	Avg	Long	Queue
completed	es.thread_pool.completed	Sum	Long	Total completed
active	es.thread_pool.active	Avg	Long	Active
min	es.thread_pool.min	Min	Long	Min
rejected	es.thread_pool.rejected	Sum	Long	Total rejected
queue size	es.thread_pool.queue.size	Avg	Long	Queue size
size	es.thread_pool.size	Avg	Long	Size
max	es.thread_pool.max	Max	Long	Max
largest	es.thread_pool.largest	Max	Long	Largest
flush count (all)	es.indexing.flush.total	Sum	Long	Total flush count on all (primary and replica) shards

Metric Name	Key	Agg	Type	Description
refreshes count (prim)	es.indexing.refreshes.count	Sum	Long	refresh count on primary shards
docs count (prim)	es.indexing.merges.docs.count	Sum	Long	merge docs count on primary shards
refreshes count (all)	es.indexing.ddsrefreshes.total	Sum	Long	refresh count on all (primary and replica) shards
merge count (all)	es.indexing.merges.total	Sum	Long	merge count on all (primary and replica) shards

Metric Name	Key	Agg	Type	Description
flush time (all)	es.indexing.flush.time	Sum	Long	flush time on all (primary and replica) shards
flush count (prim)	es.indexing.flush.count	Sum	Long	flush count on primary shards
indexed docs (prim)	es.indexing.docs	Sum	Long	docs indexed on primary shards
merge time (all)	es.indexing.merge.time	Sum	Long	merge time on all (primary and replica) shards

Metric Name	Key	Agg	Type	Description
indexed docs (all)	es.indexing.docs.total	Sum	Long	total docs indexed on all (primary and replica) shards
flush time (prim)	es.indexing.flush.time	Sum	Long	flush time on primary shards
refreshes time (prim)	es.indexing.refresh.time	Sum	Long	refresh time on primary shards
merge time (prim)	es.indexing.merge.time	Sum	Long	merge time on primary shards

Metric Name	Key	Agg	Type	Description
docs count (all)	es.indexing.merges.docs.total	Sum	Long	docs count on all (primary and replica) shards
merge count (prim)	es.indexing.merges.total	Sum	Long	merge count on primary shards
refresh time (all)	es.indexing.refreshes.total	Sum	Long	refresh time on all (primary and replica) shards
docs size (all)	es.indexing.merges.docs.size.total	Sum	Long	docs size on all (primary and replica) shards

Metric Name	Key	Agg	Type	Description
docs size (prim)	es.indexing.merges.docs.size	Sum	Long	docs size on primary shards
delete total (prim)	es.indexing.deletes.docs.deleted	Sum	Long	docs deleted on primary shards
delete total (all)	es.indexing.deletes.docs.total	Sum	Long	docs deleted on all (primary and replica) shards