Elasticsearch Training
Session 7

Rajan Manickavasagam

Agenda

- Configuration
- Guidelines for Production
- Administration API's
- Snapshot + Restore

Configuration

- Configuration is set in 2 main files –
  - elasticsearch.yml
  - logging.yml

Configuration

- Configuration is set in 2 main files –
    - elasticsearch.yml
    - logging.yml

Guidelines for Production

- Server
  - Use SSD for fast indexing & searching.
  - Look at RAID for performance improvement and use elasticsearch replicas for HA.
- Operating System
  - Set vm.swappiness to 1. This reduces the aggressiveness by which the OS swaps memory.
  - Lucene uses lot of files and elasticsearch uses lot of sockets. All this require file descriptors. Ideally, keep file descriptors to 64,000. If not possible, set to at least 32,000. Verify using ‘curl localhost:9200/_nodes/process’.
  - Have as much as system cache. This is used for sorting, faceting & filter cache.
- JVM
  - Do not allocate more than 32 GB per JVM (due to pointer compression).
  - Set ES_HEAPSIZE to set the JVM memory. Set memory to 50% of total on a server. The remaining memory is left to the system cache, which is good (since Lucene internally uses the system cache).
  - JVM can be monitored from ‘http://localhost:9200/_nodes/stats/java’

Guidelines for Production

- Elasticsearch
  - Disable scripting in production for security reasons.
  - Disable multicast (as it is chattier) and enable unicast hosts for distributed nodes.
  - Use minimum master configuration to prevent "multiple masters" scenario when nodes disconnect.
  - Disable shard rebalancing.
  - Separate the thread pools for indexing, search, bulk operations, percolate, refresh, merge etc.
  - Set bootstrap.mlockall to true. This allows JVM to lock all memory.
  - Field data can be memory intensive.
  - Bloom filters can have significant impact on memory footprint.
  - If using synonyms are modified, all data needs to be reindexed. Consider keeping separate analyzer for search and indexing. Use synonym in the search analyzer.
  - If input document being indexed is large, consider disabling _source field.
  - Caching query filters increases performance but uses a lot of memory.
  - Register bitsets using Warmer API.
  - Each shard has overheads - lucene, memory, storage and file descriptors.
  - Use Marvel for monitoring elasticsearch.
  - Explain API is available for understanding queries / results. Use it only for debugging and not in production.

Guidelines for Production

- Client
  - Client machines should also have same version of Java (as server) to reduce risk of incompatibility.
  - Use long lived HTTP connections, short lived connections can cause load on opening/closing sockets.
- Cloud
  - Additional recommendations for deploying on AWS are:
    - Use Large instances.
    - Minimum recommendation is type is m1.xlarge.
    - If using EBS, use provisioned IOPS.
    - Run elasticsearch cluster on private/local IP’s.
    - Use a reverse proxy or Shield plugin to secure elasticsearch.

Administration API’s

- Cat API
  - Get information in readable format.

- Node Stats API
  - Provides information about a node or a collection.

Administration API’s

- Cluster API
  - Health: Provides health of a cluster.
  - State: Provides detailed stats of cluster.
  - Stats: Provides basic index metrics and plugins.
  - Pending Tasks: View pending activities.
  - Reroute: Allocate or move shards.
  - Update: Update cluster wide settings (transient/persistent).

Snapshot + Restore

- Define a backup

- Snapshot API – Take snapshots to the backup location.

- Restore API – Restore from a snapshot.