Errors (**A**irways)

Utilization (**B**reathing)

Saturation (**C**irculation)

Sensibility* (**D**isability)

Historical (**E**xposure)

Log:

- *ERROR*
- HTTP codes: *400 | 429 | 50x*

Diagnostic / API:

- CAT Threadpool > *rejected*
- Node Stats
  - Circuit Breakers
- e.g. Plugins
  - Cluster Health
  - ILM Explain > *ERROR*

E.g.

- *status:red* from *node-left*
- bad *elasticsearch.yml* settings

Log:

- *trigger G1GC*
- *timed out*
- Slow Logs

Diagnostic / API:

- CAT Nodes
- CAT Allocation
- CAT Pending Tasks
- CAT Tasks > long-running
- ILM Explain > transition steps

E.g.

- *heap:>75% triggers GC*
- *cpu:>100% may be stuck*
- *disk:>85% hit* watermark
- ILM stuck on migration / snapshot step

Log:

- *lagging | retry count exceeded*
- *warn threshold*
- *throttled | queue capacity*

Diagnostic / API:

- CAT Threadpool > *queue*
- CAT Tasks > quantity
- Hot Threads (KB) > *cpu vs other*
- long API response durations

E.g.

- Node Hot Spotting ingest / search

---

* gets tribal knowledge fast; has much broader scope because not just break/fix

When in doubt, check it out

- Cluster Health

- CAT Nodes > *cpu, heap.percent*
- CAT Allocation > *disk.percent, shards*

- CAT Pending Tasks (should be empty)
- CAT Tasks > long-running, quantity
- CAT Threadpool > *queue*

Down

Impaired

Performance

RCA/Improve

Errors
(**A**irways)

Log:

- *node-left* | *disconnect* | *exitCode*
- *InternalServerError*
- *OOM* | *OutOfMemoryError*
- *CircuitBreakingException*
- *ERROR*
  - *security initialization failed*
  - *IllegalStateException*
  - *mapper_parsing_exception*
- HTTP codes: *400* | *429* | *50x*

Diagnostic / API:

- CAT Threadpool > *rejected*
- Node Stats
  - Circuit Breakers
  - Coordinating Rejections
- e.g. Plugins
  - Cluster Health
  - ILM Explain > *ERROR*

E.g.

- *status:red* from *node-left*
- bad *elasticsearch.yml* settings

Utilization
(**B**reathing)

Log:

- *trigger G1GC*
- *environment is not locked*
- *timed out*
- *corrupt*
- Slow Logs

Diagnostic / API:

- CAT Nodes
- CAT Allocation
- CAT Pending Tasks
- CAT Tasks > long-running
- Node Hot Threads
- ILM Explain > transition steps

E.g.

- *heap:>75% triggers GC*
- *cpu:>100% probably stuck*
- *disk:>85% hit watermark*
- *disk.indices << disk.used*
- ILM stuck on migration / snapshot step

Saturation
(**C**irculation)

Log:

- *lagging* | *retry count exceeded*
- *warn threshold*
- *throttled* | *queue capacity*

Diagnostic / API:

- CAT Threadpool > *queue*
- CAT Tasks > quantity
  - GET Tasks > *description*
- Node Stats
  - Memory Pressure
  - Indexing Pressure
- CAT Nodes > *load_Xm*
- Hot Threads (KB) > *cpu vs other*
- long API response durations

E.g.

- Mapping Explosion
- Node Hot Spotting ingest / search
- Future Dates in Frozen indices causing searches to hit _partial-*_ indices increasing task time

Sensibility*
(**D**isability)

Log:

- *compressed ordinary object pointers*

Diagnostic / API:

- Index Settings
  - *.mapping.total_fields.limit*
  - *.refresh_interval: -1*
- Cluster Settings
  - *node_concurrent_recoveries*
  - *max_shards_per_node*
  - *search.max_buckets*
- Index Templates referencing Node Attributes for data temperatures while using ILM

E.g.

- Searches reserve expected heap before starting, so don't arbitrarily set high buckets

* gets tribal knowledge fast; has much broader scope because not just break/fix

Historical
(**E**xposure)

Log: (see earlier columns)

Diagnostic / API:

- Index Stats
- Node Stats
- Node Usage
- CAT Recovery

E.g. valid concern but no longer live

- an expensive search hitting cold nodes caused Cluster State syncing to temporarily slow down
- a shard on a node had experienced hot spotting until index rolled over and new shards distributed better