

API

<a href="#">doc</a>		
<b>DOC</b>	<b>API</b>	<b>DIAG</b>
<a href="#">Node Stats API</a>	curl -XGET localhost:9600/_node/stats	logstash_node_stats.json
<a href="#">Node Info API</a>	curl -XGET localhost:9600/_node	logstash_node.json
<a href="#">Node Hot Threads</a>	curl -XGET localhost:9600/_node/hot_threads?pretty	logstash_nodes_hot_threads.json
<a href="#">Plugins Info</a>	curl -XGET localhost:9600/_node/plugins?pretty	logstash_plugins.json
<a href="#">Version</a>	curl -XGET localhost:9600?pretty	logstash_version.json

DIAG

```
Run (code)

$ curl -L -O https://github.com/elastic/support-diagnostics/releases/download/v8.4.0/diagnostics-8.4.0-dist.zip
$ unzip diagnostics-8.4.0-dist.zip
$ cd diagnostics-8.4.0
$
$ # choose between either
$ sudo ./diagnostics.sh --type logstash --host localhost
$ ./diagnostics.sh --type logstash-local --host 10.0.0.20 --port 9600
```

LOG

```
doc

$ # override logging level
$ curl -XPUT -s http://localhost:9600/_node/logging -H 'Content-Type: application/json' -d '{ "logger.org.logstash": "DEBUG", "logger.logstash": "DEBUG" }'
$ # reset logging to config
$ curl -s 'http://localhost:9600/_node/logging/reset?pretty' -XPUT
```

JQ

Using Bash [jq](#)

PIPELINES

CONFIG

```
$ cat logstash_node.json | jq --sort-keys '.pipelines|to_entries|map_values(.value+(pipeline:.key))'
```

ERROR

```
$ cat logstash_node_stats.json | jq --sort-keys '.pipelines|to_entries[]|select(.value.events.in>0)|{pipeline:.key, events_in:.events.in, events_out:.events.out, failures:.reloads.failures, last_failure:.reloads.last_failure_timestamp, last_error:.reloads.last_error, successes:.reloads.successes, last_success:.reloads.last_success_timestamp}'
```

DURATION

```
duration/events & events/duration

$ cat logstash_node_stats.json | jq -c '.pipelines|to_entries[]|select(.value.events.in>0)|{pipeline:.key,events_ct:.value.events.in,events_dur:.value.events.duration_in_millis, events_avg:(.value.events.duration_in_millis/.value.events.in), out_per_ms:(.value.events.out/.value.events.duration_in_millis)}'

obvious duration issues (events_avg>1)

$ cat logstash_node_stats.json | jq '.pipelines|to_entries[]|select(.value.events.in>0)|select(.value.events.duration_in_millis / .value.events.in > 1)|{pipeline:.key,events_ct:.value.events.in,events_dur:.value.events.duration_in_millis, events_avg:(.value.events.duration_in_millis/.value.events.in)}'
```

PLUGINS

```
Pipeline>plugin>name

$ cat logstash_node_stats.json | jq '.pipelines|to_entries[]|.key as $pi|.value.plugins|to_entries[]|.key as $pl|.value|map_values(+(pipeline:$pi, plugin:$pl, out_per_ms:(try (.events.out/.events.duration_in_millis) catch 0), in_per_ms:(try (.events.in/.events.duration_in_millis) catch 0), duration_ms:.events.duration_in_millis, in:.events.in, out:.events.out))|del(.[].events)|sort_by(.pipeline,.plugin,-.out_per_ms)'
```

SUPPORT MESSAGING

**Context:** A few questions to begin:

1. Is this a new setup or configuration that you're trying to implement?
2. Was this working as expected previously and then stopped? If so, when did the issue start?
3. Kindly outline any recent changes (in config/traffic) that could potentially influence investigation.
4. Kindly outline ETL pipeline architecture (e.g. "FluentDB > Logstash (1st) > Kafka > Logstash (2nd) > Elasticsearch").

**Config:** Kindly attach the following for review: `pipelines.yml` (and/or sub-pipelines), `logstash.yml`, `logstash.conf`.

**Performance:** Kindly attach a [Logstash Diagnostic](#).