Data and Access Monitoring (DAM) Requirements

This document is to provide a baseline understanding of how Elasticsearch meets the requirements of Data and Access Monitoring (DAM). It walks through required settings changes. Then it walks the user through creating some sample data, how to configure the environment to generate audit/log events for the sample data, and where to find the required information from the log output.

Required Steps to Configure Auditing on Elasticsearch

Node Configuration For Auditing

Elasticsearch (elasticsearch.yml)

```
xpack.security.audit.enabled: true
xpack.security.audit.logfile.events.emit_request_body: true
xpack.security.audit.logfile.emit_node_host_address: true
xpack.security.audit.logfile.emit_node_host_name: true
```

Index Configuration for Queries

Setup your index in Elasticsearch to log slow queries. This would normally be tuned for your specific use case, but for the purposes of meeting DAM requirements we can set this to a very low number to capture all queries.

```
PUT /YOUR_INDEX_NAME_HERE/_settings
{
   "index.search.slowlog.threshold.query.warn": "10s",
    "index.search.slowlog.threshold.query.info": "5s",
    "index.search.slowlog.threshold.query.debug": "2s",
    "index.search.slowlog.threshold.query.trace": "1ms",
    "index.search.slowlog.threshold.fetch.warn": "1s",
    "index.search.slowlog.threshold.fetch.info": "800ms",
    "index.search.slowlog.threshold.fetch.debug": "200ms",
    "index.search.slowlog.threshold.fetch.trace": "1ms",
    "index.search.slowlog.level": "trace"
}
```

Log File Names

Where audit events get logged to: **elasticsearch_audit.json**

Where slow queries get logged to: **elasticsearch_index_search_slowlog.json**

Data Setup For Example

Load data into Elasticsearch so audit and log data can be generated

```
# Use the bulk API
POST /orders/_bulk
{ "index" : { "_id" : "1" } }
{"first_name":"kimchy","phone":"111-111-1111","sale_amount":34.25,"post_date":"2019-11-15T14:12:12","message":"trying out Elasticsearch"}
{ "index" : { "_id" : "2" } }
{"first_name":"kimchy","phone":"111-111-1111","sale_amount":41.26,"post_date":"2019-12-15T14:12:12","message":"trying out Elasticsearch"}
{ "index" : { "_id" : "3" } }
{"first_name":"bran","phone":"222-222-2222","sale_amount":40.26,"post_date":"2019-11-16T14:12:12","message":"trying out Elasticsearch"}
{ "index" : { "_id" : "4" } }
{"first_name":"john","phone":"333-333-3333","sale_amount":56.26,"post_date":"2019-10-15T14:12:12","message":"trying out Elasticsearch"}
{ "index" : { "_id" : "5" } }
{"first_name":"john","phone":"333-333-3333","sale_amount":33.26,"post_date":"2019-11-15T14:12:12","message":"trying out Elasticsearch"}
{ "index" : { "_id" : "6" } }
{"first_name":"jane","phone":"444-444-4444","sale_amount":33.26,"post_date":"2019-09-15T14:12:12","message":"trying out Elasticsearch"}
{ "index" : { "_id" : "7" } }
{"first_name":"jane","phone":"444-444-4444","sale_amount":12.46,"post_date":"2019-08-15T14:12:12","message":"trying out Elasticsearch"}
{ "index" : { "_id" : "8" } }
{"first_name":"rakesh","phone":"555-555-5555","sale_amount":14.55,"post_date":"2019-09-16T14:12:12","message":"trying out Elasticsearch"}
```

Queries Ran

This is a basic query that looks for the first name of “kimchy” in the orders data

```
GET /orders/_search`
{
   "query":{
      "bool":{
         "filter":{
```

```
            "term":{
               "first_name":"kimchy"
            }
         }
      }
   }
}
```

To get slower queries we execute a more complicated query so that the query can take over 1ms and get logged

```
GET /orders/_search
{
   "query":{
      "bool":{
         "filter":{
            "range":{
               "sale_amount":{
                  "gte":20.0
               }
            }
         }
      }
   },
   "collapse":{
      "field":"phone.keyword"
   },
   "aggs":{
      "phone_number":{
         "terms":{
            "field":"phone.keyword"
         },
         "aggs":{
            "avg_sales":{
               "avg":{
                  "field":"sale_amount"
               }
            }
         }
      }
   }
}
```

DAM Requirements

Successful logins

All Elasticsearch interactions are over the HTTPS protocol. HTTPS by its nature is a stateless protocol and as such it does not have sessions which have traditional logins. Credentials are provided with every call therefore to log all successful logins one has to capture every single interaction with the system to satisfy this requirement. This is handled by capturing every single audit event from the elasticsearch_audit.json log file with an event_type of access granted.


```
{
   "type":"audit",
   "timestamp":"2020-04-09T00:00:00,940-0400",
   "node.id":"sE6PeshwT9Ohjv9xWPnyiA",
   "host.name":"127.0.0.1",
   "host.ip":"127.0.0.1",
   "event.type":"transport",
   "event.action":"access_granted",
   "user.name":"kibana",
   "user.realm":"reserved",
   "user.roles":[
      "kibana_system"
   ],
   "origin.type":"rest",
   "origin.address":"127.0.0.1:49579",
   "request.id":"ymktsvK8SRWqtCrpnwBXXQ",
   "action":"indices:data/read/get[s]",
   "request.name":"GetRequest",
   "indices":[
      ".kibana"
   ]
}
```


First time access

Not Applicable since Elasticsearch only uses HTTPs. Every call to Elasticsearch is a first time access.

Failed logins

Elasticsearch


```
{
   "type":"audit",
   "timestamp":"2020-04-08T13:13:13,897-0400",
   "node.id":"sE6PeshwT9Ohjv9xWPnyiA",
   "host.name":"127.0.0.1",
   "host.ip":"127.0.0.1",
   "event.type":"rest",
   "event.action":"authentication_failed",
   "user.name":"elastic",
   "origin.type":"rest",
   "origin.address":"127.0.0.1:49519",
   "url.path":"/orders/_search",
   "url.query":"pretty",
   "request.method":"GET",
   "request.body":"\n{\n    \"query\" : {\n        \"term\" : { \"first_name\" : \"kimchy\" }\n    }\n}\n",
   "request.id":"i6sUUga4TU-BRZStAYe0kA"
}
```

Attributes to be logged

User Id


```
{
   "type":"audit",
   "timestamp":"2020-04-08T13:13:13,897-0400",
   "node.id":"sE6PeshwT9Ohjv9xWPnyiA",
   "host.name":"127.0.0.1",
   "host.ip":"127.0.0.1",
   "event.type":"rest",
   "event.action":"authentication_failed",
   "user.name":"elastic",
   "origin.type":"rest",
   "origin.address":"127.0.0.1:49519",
   "url.path":"/orders/_search",
   "url.query":"pretty",
   "request.method":"GET",
   "request.body":"\n{\n    \"query\" : {\n        \"term\" : { \"first_name\" :
\"kimchy\" }\n    }\n}\n",
   "request.id":"i6sUUga4TU-BRZStAYe0kA"
}
```


Client hostname or source IP


```
{
   "type":"audit",
   "timestamp":"2020-04-08T13:13:13,897-0400",
   "node.id":"sE6PeshwT9Ohjv9xWPnyiA",
   "host.name":"127.0.0.1",
   "host.ip":"127.0.0.1",
   "event.type":"rest",
   "event.action":"authentication_failed",
   "user.name":"elastic",
   "origin.type":"rest",
   "origin.address":"127.0.0.1:49519",
   "url.path":"/orders/_search",
   "url.query":"pretty",
   "request.method":"GET",
   "request.body":"\n{\n    \"query\" : {\n        \"term\" : { \"first_name\" :
\"kimchy\" }\n    }\n}\n",
   "request.id":"i6sUUga4TU-BRZStAYe0kA"
}
```


Timestamp of when it happened


```
{
   "type":"audit",
   "timestamp":"2020-04-08T13:13:13,897-0400",
   "node.id":"sE6PeshwT9Ohjv9xWPnyiA",
   "host.name":"127.0.0.1",
   "host.ip":"127.0.0.1",
   "event.type":"rest",
   "event.action":"authentication_failed",
   "user.name":"elastic",
   "origin.type":"rest",
   "origin.address":"127.0.0.1:49519",
   "url.path":"/orders/_search",
   "url.query":"pretty",
   "request.method":"GET",
   "request.body":"\n{\n    \"query\" : {\n        \"term\" : { \"first_name\" :
\"kimchy\" }\n    }\n}\n",
```

```
   "request.id":"i6sUUga4TU-BRZStAYe0kA"
}
```


What they logged in to/attempted to log in to

Orders is the index in this example that contains the data.


```
{
   "type":"audit",
   "timestamp":"2020-04-08T13:13:13,897-0400",
   "node.id":"sE6PeshwT9Ohjv9xWPnyiA",
   "host.name":"127.0.0.1",
   "host.ip":"127.0.0.1",
   "event.type":"rest",
   "event.action":"authentication_failed",
   "user.name":"elastic",
   "origin.type":"rest",
   "origin.address":"127.0.0.1:49519",
   "url.path":"/orders/_search",
   "url.query":"pretty",
   "request.method":"GET",
   "request.body":"\n{\n    \"query\" : {\n        \"term\" : { \"first_name\" :
\"kimchy\" }\n    }\n}\n",
   "request.id":"i6sUUga4TU-BRZStAYe0kA"
}
```


Query Operations to be logged

What query/operation was run

Denied Requests from audit logs


```
{
   "type":"audit",
   "timestamp":"2020-04-08T11:57:04,414-0400",
   "node.id":"sE6PeshwT9Ohjv9xWPnyiA",
   "host.name":"127.0.0.1",
   "host.ip":"127.0.0.1",
   "event.type":"rest",
   "event.action":"anonymous_access_denied",
   "origin.type":"rest",
   "origin.address":"127.0.0.1:64845",
   "url.path":"/orders/_search",
   "url.query":"pretty",
   "request.method":"GET",
   "request.body":"\n{\n \"query\": {\n        \"term\":{ \"user\":\"kimchy\"
}\n}\n}\n",
   "request.id":"dZuyhOmxS-yvPgzYCXXgWg"
}
```


Query from slow logs


```
{
   "type":"index_search_slowlog",
   "timestamp":"2020-04-09T10:31:21,571-04:00",
   "level":"WARN",
   "component":"i.s.s.q.kSD5uMbYSg6t9EE-ViEL7Q",
   "cluster.name":"elasticsearch",
   "node.name":"shawn-mbp.local",
   "message":"[orders][0]",
   "took":"15ms",
   "took_millis":"15",
```

```
   "total_hits":"6 hits",
   "types":"[]",
   "stats":"[]",
   "search_type":"QUERY_THEN_FETCH",
   "total_shards":"1",

"source":"{\"query\":{\"bool\":{\"filter\":[{\"range\":{\"sale_amount\":{\"from\
":30.0,\"to\":null,\"include_lower\":true,\"include_upper\":true,\"boost\":1.0}}
}],\"adjust_pure_negative\":true,\"boost\":1.0}},\"aggregations\":{\"phone_numbe
rs\":{\"terms\":{\"field\":\"phone.keyword\",\"size\":3,\"min_doc_count\":1,\"sh
ard_min_doc_count\":0,\"show_term_doc_count_error\":false,\"order\":[{\"_count\"
:\"desc\"},{\"_key\":\"asc\"}]}}}}",
   "cluster.uuid":"4lKGoY3xR3S_nKrw7qsSZg",
   "node.id":"sE6PeshwT9Ohjv9xWPnyiA"
}
```


Who ran the query


```
{
   "type":"audit",
   "timestamp":"2020-04-08T12:36:48,365-0400",
   "node.id":"sE6PeshwT9Ohjv9xWPnyiA",
   "host.name":"127.0.0.1",
   "host.ip":"127.0.0.1",
   "event.type":"transport",
   "event.action":"access_granted",
   "user.name":"elastic",
   "user.realm":"reserved",
   "user.roles":[
      "superuser"
   ],
   "origin.type":"rest",
   "origin.address":"127.0.0.1:65520",
   "request.id":"CjQ62OnaS4Kcg-U7nFD4hg",
   "action":"indices:data/read/search",
   "request.name":"SearchRequest",
   "indices":[
      "orders"
   ]
}
```


What time the query was run

Denial


```
{
   "type":"audit",
   "timestamp":"2020-04-08T11:57:04,414-0400",
   "node.id":"sE6PeshwT9Ohjv9xWPnyiA",
   "host.name":"127.0.0.1",
   "host.ip":"127.0.0.1",
   "event.type":"rest",
   "event.action":"anonymous_access_denied",
   "origin.type":"rest",
   "origin.address":"127.0.0.1:64845",
   "url.path":"/orders/_search",
   "url.query":"pretty",
   "request.method":"GET",
   "request.body":"\n{\n \"query\": {\n        \"term\":{ \"user\":\"kimchy\"
}\n}\n}\n",
```

```
   "request.id":"dZuyhOmxS-yvPgzYCXXgWg"
}
```


Authorized


```
{
   "type":"audit",
   "timestamp":"2020-04-08T12:36:48,365-0400",
   "node.id":"sE6PeshwT9Ohjv9xWPnyiA",
   "host.name":"127.0.0.1",
   "host.ip":"127.0.0.1",
   "event.type":"transport",
   "event.action":"access_granted",
   "user.name":"elastic",
   "user.realm":"reserved",
   "user.roles":[
      "superuser"
   ],
   "origin.type":"rest",
   "origin.address":"127.0.0.1:65520",
   "request.id":"CjQ62OnaS4Kcg-U7nFD4hg",
   "action":"indices:data/read/search",
   "request.name":"SearchRequest",
   "indices":[
      "orders"
   ]
}
```


Query run time

Queries are recorded. This is configurable by setting thresholds on query time and log level.


```
{
   "type":"index_search_slowlog",
   "timestamp":"2020-04-09T10:31:21,571-04:00",
   "level":"WARN",
   "component":"i.s.s.q.kSD5uMbYSg6t9EE-ViEL7Q",
   "cluster.name":"elasticsearch",
   "node.name":"shawn-mbp.local",
   "message":"[orders][0]",
   "took":"15ms",
   "took_millis":"15",
   "total_hits":"6 hits",
   "types":"[]",
   "stats":"[]",
   "search_type":"QUERY_THEN_FETCH",
   "total_shards":"1",

"source":"{\"query\":{\"bool\":{\"filter\":[{\"range\":{\"sale_amount\":{\"from\
":30.0,\"to\":null,\"include_lower\":true,\"include_upper\":true,\"boost\":1.0}}
}],\"adjust_pure_negative\":true,\"boost\":1.0}},\"aggregations\":{\"phone_numbe
rs\":{\"terms\":{\"field\":\"phone.keyword\",\"size\":3,\"min_doc_count\":1,\"sh
ard_min_doc_count\":0,\"show_term_doc_count_error\":false,\"order\":[{\"_count\"
:\"desc\"},{\"_key\":\"asc\"}]}}}}",
   "cluster.uuid":"4lKGoY3xR3S_nKrw7qsSZg",
   "node.id":"sE6PeshwT9Ohjv9xWPnyiA"
}
```


See https://www.elastic.co/guide/en/elasticsearch/reference/current/index-modules-slowlog.html for more information

What the query was run against

Denial


```
{
```

```
   "type":"audit",
   "timestamp":"2020-04-08T11:57:04,414-0400",
   "node.id":"sE6PeshwT9Ohjv9xWPnyiA",
   "host.name":"127.0.0.1",
   "host.ip":"127.0.0.1",
   "event.type":"rest",
   "event.action":"anonymous_access_denied",
   "origin.type":"rest",
   "origin.address":"127.0.0.1:64845",
   "url.path":"/orders/_search",
   "url.query":"pretty",
   "request.method":"GET",
   "request.body":"\n{\n \"query\": {\n        \"term\":{ \"user\":\"kimchy\"
}\n}\n}\n",
   "request.id":"dZuyhOmxS-yvPgzYCXXgWg"
}
```


Authorized


```
{
   "type":"audit",
   "timestamp":"2020-04-08T12:36:48,365-0400",
   "node.id":"sE6PeshwT9Ohjv9xWPnyiA",
   "host.name":"127.0.0.1",
   "host.ip":"127.0.0.1",
   "event.type":"transport",
   "event.action":"access_granted",
   "user.name":"elastic",
   "user.realm":"reserved",
   "user.roles":[
      "superuser"
   ],
   "origin.type":"rest",
   "origin.address":"127.0.0.1:65520",
   "request.id":"CjQ62OnaS4Kcg-U7nFD4hg",
   "action":"indices:data/read/search",
   "request.name":"SearchRequest",
   "indices":[
      "orders"
   ]
}
```


Where was it run from


```
{
   "type":"audit",
   "timestamp":"2020-04-08T13:13:13,897-0400",
   "node.id":"sE6PeshwT9Ohjv9xWPnyiA",
   "host.name":"127.0.0.1",
   "host.ip":"127.0.0.1",
   "event.type":"rest",
   "event.action":"authentication_failed",
   "user.name":"elastic",
   "origin.type":"rest",
   "origin.address":"127.0.0.1:49519",
   "url.path":"/orders/_search",
   "url.query":"pretty",
   "request.method":"GET",
   "request.body":"\n{\n    \"query\" : {\n        \"term\" : { \"first_name\" :
\"kimchy\" }\n    }\n}\n",
```

```
    "request.id":"i6sUUga4TU-BRZStAYe0kA"
}
```


Number of records returned

Denial

Number of records cannot be returned for denials.

Authorized


```
{
    "type":"index_search_slowlog",
    "timestamp":"2020-04-09T10:31:21,571-04:00",
    "level":"WARN",
    "component":"i.s.s.q.kSD5uMbYSg6t9EE-ViEL7Q",
    "cluster.name":"elasticsearch",
    "node.name":"shawn-mbp.local",
    "message":"[orders][0]",
    "took":"15ms",
    "took_millis":"15",
    "total_hits":"6 hits",
    "types":"[]",
    "stats":"[]",
    "search_type":"QUERY_THEN_FETCH",
    "total_shards":"1",

"source":"{\"query\":{\"bool\":{\"filter\":[{\"range\":{\"sale_amount\":{\"from\
":30.0,\"to\":null,\"include_lower\":true,\"include_upper\":true,\"boost\":1.0}}
}],\"adjust_pure_negative\":true,\"boost\":1.0}},\"aggregations\":{\"phone_numbe
rs\":{\"terms\":{\"field\":\"phone.keyword\",\"size\":3,\"min_doc_count\":1,\"sh
ard_min_doc_count\":0,\"show_term_doc_count_error\":false,\"order\":[{\"_count\"
:\"desc\"},{\"_key\":\"asc\"}]}}}}",
    "cluster.uuid":"4lKGoY3xR3S_nKrw7qsSZg",
    "node.id":"sE6PeshwT9Ohjv9xWPnyiA"
}
```


Global Search Timeout

Individual searches can have a timeout as part of the Request Body Search. Since search requests can originate from many sources, Elasticsearch has a dynamic cluster-level setting for a global search timeout that applies to all search requests that do not set a timeout in the request body. These requests will be cancelled after the specified time using the mechanism described in the following section on Search Cancellation. Therefore the same caveats about timeout responsiveness apply.

The setting key is `search.default_search_timeout` and can be set using the Cluster update settings endpoints. The default value is no global timeout. Setting this value to `-1` resets the global search timeout to no timeout.

https://www.elastic.co/guide/en/elasticsearch/reference/7.6/search.html#global-search-timeout