Meeting compliance regulations with Search Guard audit logging

Jochen Kressin · 2017-06-09

Audit logging makes it possible to keep a record of everything that is going on in your cluster. Search Guard provides a sound, bullet-proof, and flexible Audit Log module that enables you to record any activity in your cluster, find anomalies, and, most importantly, take action.

What is Audit Logging?

"An **audit trail** (also called **audit log**) is a security-relevant chronological record, set of records, and/or destination and source of records that provide documentary evidence of the sequence of activities that have affected at any time a specific operation, procedure, or event."

(Source: https://en.wikipedia.org/wiki/Audit_trail)

Log what's relevant and stay compliant

To put it in simpler words, audit logging allows you to record any activity that is going on in your cluster. This could be as simple as recording all failed login attempts, but it's not limited to that. Search Guard can record and store any kind of activity, up to and including valid, successful requests. Supported audit log categories include:

- FAILED_LOGIN
  - the provided credentials of a request could not be validated, most likely because the user does not exist or the password is incorrect.

- MISSING_PRIVILEGE
  - an attempt was made to access Elasticsearch, but the user does not have the required permissions.
- SSL_EXCEPTION
  - an attempt was made to access Elasticsearch without a valid SSL/TLS certificate.
- BAD_HEADERS
  - an attempt was made to spoof a request to Elasticsearch with Search Guard internal headers.
- SG_INDEX_ATTEMPT
  - an attempt was made to access the Search Guard internal user and privileges index without a valid admin TLS certificate.
- AUTHENTICATED
  - represents a successful request to Elasticsearch.

Depending on your security and/or compliance requirements, you can choose which events you want to record. Only a few? All? It's totally up to you.

What is being logged?

Search Guard offers two log levels, basic and extended logging.

The basic log level, which is the default, already offers a ton of useful information per logged message. Depending on the nature of the request, for example, if it's a request on HTTP or transport level, the message contains:

- UTC timestamp of the event
- Origin IP and host
- Audit reason, e.g. failed log in
- Username
- Used TLS certificates
- Node name where the message occurred
- ... and much more ...

The extended logging goes even further by adding:

- The original query
- All original indices and aliases
- All actually affected and resolved indices

Even if the original request is a composite or bulk request, Search Guard will resolve all indices affected by the request, and list them in the extended log message. This gives you the ultimate tool to track exactly what is going on in your cluster. This helps you stay compliant with internal security policies and regulations like HIPAA, PCI DSS, FISMA, and ISO.

Where do the audit logs go?

Elasticsearch is distributed in nature, so writing the audit events to the log file of each node does not really make sense. Instead, you want to use a central storage where all nodes write to, and which you can use to analyze the log events.

Logging to Elasticsearch

Guess what, we already have such a system in place, and it's called Elasticsearch. Search Guard can write the audit messages either to the same cluster, or a remote Elasticsearch cluster. The latter can be used to ship the log events off -premise, making it hard for an attacker to cover his tracks. You can then use any tool in the Elastic ecosystem to analyze the messages and generate alerts, should you find something suspicious.

Logging to external SIEM and monitoring systems

There are already many Security Information and Event Management (SIEM) systems out there, and you probably already have one in place. Search Guars supports shipping events to web hooks, so as long as your system provides any HTTP(S) endpoint, Search Guard can ship to it! This also includes traditional monitoring systems like Nagios or Icinga.

Custom storage

If your storage solution of choice does not support webhooks but uses some custom protocol, for example, you can always write your own storage implementation! Search Guard provides an extension point in the audit log module where you can plug in your own storage implementation. It's totally up to you what to do with the audit events. Need to encrypt the messages before storing them? Need to convert them to a special, in-house JSON format? If you can code it, Search Guard supports it.

Summary

Using the Search Guard audit log module arms you with a powerful tool to record any suspicious activity in your Elasticsearch cluster. You can configure the event categories and the log level to adapt the messages to exactly your requirements. Audit events can be stored in an Elasticsearch cluster, also off-premise, or in any SIEM or monitoring system that supports webhooks.

Image: shutterstock / LeoWolfert

This article was published on the Search Guard blog: https://search-guard.com/blog/audit-logging-elasticsearch-compliance/