Search Guard Helpful Hints: Limit access to most recent Elasticsearch indices

Jochen Kressin · 2020-10-15

This is the first article in our "Helpful Hints" series where we will describe how to implement real-world use cases step-by-step. Helpful Hints will be published bi-weekly and are quick 2-3 minute reads.

Elasticsearch date math expressions

Elasticsearch supports date math expressions in index names. You can use these expressions when creating an index and when querying indices.

A date math index name has the following format:

```
<static_name{date_math_expr{date_format|time_zone}}>
```

As an example, if today is the 21st of October 2020, the following index name:

```
<logstash-{now/M{yyyy.MM}}>
```

Would expand to:

```
logstash-2020.10
```

See the official Elasticsearch docs for more examples on Date/Math expressions.

Date math expressions are great for querying indices that contain a date in the index name, as most logfile based indices do. Especially if you set up a daily, weekly, or monthly rolling index policy.

Using date math expressions for access control

Search Guard fully supports Elasticsearch date math index names for controlling access to data. Let's assume you have set up a logstash index pattern that contains the date and month, like:

```
logstash-2020.10
logstash-2020.09
logstash-2020.08
...
```

You want to set up a role with READ access to the logstash indices, but only allow access to logs for the current month. You can use any valid date math expression in the index_patterns section of the role definition, like:

```
sg_datemath:
  cluster_permissions:
    - SGS_CLUSTER_COMPOSITE_OPS
  index_permissions:
    - index_patterns:
      - 'logstash-{now/M{yyyy.MM}}'
      allowed_actions:
        - SGS_READ
```

The date math expression will be evaluates at runtime and, if today is 21st of October 2020, expand to *logstash-2020.10*.

Since we can define multiple index patterns per role, we can simply expand the index access to the last three months by defining the role like:

```
sg_datemath:
  cluster_permissions:
    - SGS_CLUSTER_COMPOSITE_OPS
  index_permissions:
    - index_patterns:
      - 'logstash-{now/M{yyyy.MM}}'
      - 'logstash-{now/M-1M{yyyy.MM}}'
      - 'logstash-{now/M-2M{yyyy.MM}}'
      allowed_actions:
        - SGS_READ
```

Where to go next

- Read the next helpful hint in this series (coming soon)
- Start your free Search Guard Trial today
- Deep dive into Search Guard by reading our docs

Image: Shutterstock / Irina Strelnikova

This article was published on the Search Guard blog: https://search-guard.com/blog/elasticsearch-date-math-access-control/
Search Guard is Security and Alerting for Elasticsearch and Kibana — search-guard.com · Start a free trial