Using X-Pack Monitoring with Search Guard

Cliff Staley · 2018-10-01

X-Pack monitoring is a great feature for capturing Elasticsearch cluster diagnostics. It is free and can be used together with unique security features of the Search Guard. Moreover, Search Guard already comes with predefined roles that make it easy to use X-Pack Monitoring, Alerting and Machine Learning.

Basic setup

We start with following demo-installer steps to install Elasticsearch (ES) and Search Guard:

- Download Elasticsearch.
- Install Search Guard plugin version that matches ES version installed
- Install demo configuration:
  cd /plugins/search-guard-6/tools chmod +x ./install*demo*configuration.sh
  ./install*demo*configuration.sh

Then we follow Kibana installation from demo-installer:

- Download Kibana.
- Install Search Guard Kibana plugin.
  bin/kibana-plugin install https://url/to/search-guard-kibana-plugin-.zip
- Add entries to *kibana.yml* that allow Kibana connect to secured Elasticsearch Plugin.

```
# Use HTTPS instead of HTTP
elasticsearch.url: "https://localhost:9200"

# Configure the Kibana internal server user
elasticsearch.username: "kibanaserver"
elasticsearch.password: "kibanaserver"

# Disable SSL verification because we use self-signed demo certificates
elasticsearch.ssl.verificationMode: none

# Whitelist the Search Guard Multi Tenancy Header
elasticsearch.requestHeadersWhitelist: [ "Authorization", "sgtenant" ]
```

When we start Kibana, we see an error in logs:

```
log   [18:39:46.702] [error][status][plugin:searchguard@6.4.0-14]
Status changed from uninitialized to red - X-Pack Security needs to be disabled for Search Guard
to work properly.
Please set 'xpack.security.enabled' to false in your kibana.yml
```

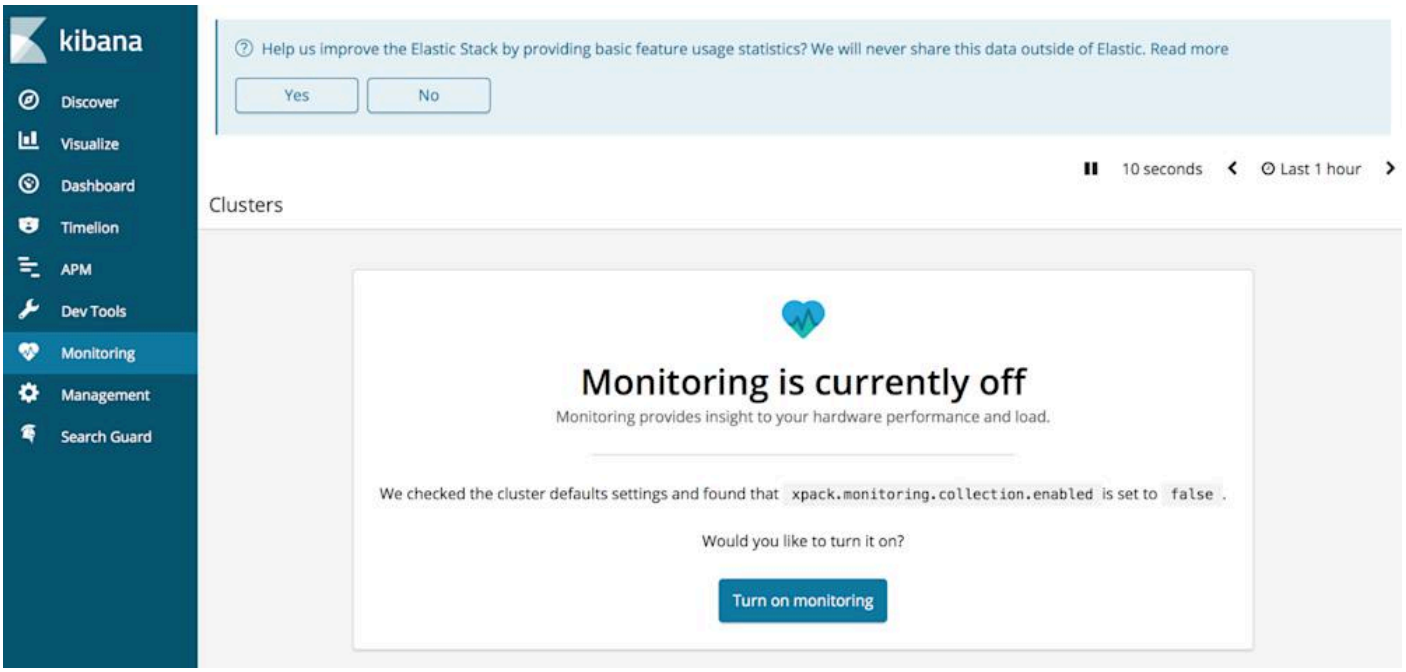
Since Elasticsearch 6.3, X-Pack is installed and switched on by default. Search Guard works great with X-Pack Monitoring, Alerting and Machine Learning, but does not work with X-Pack Security, which is reasonable.

We switch off *xpack.security* in *kibana.yml* by adding:

```
xpack.security.enabled: false
```

and start Kibana again. Note that X-Pack Security needs to be also disabled in Elasticsearch. This has been done automatically by our demo installation script.

When we log with an admin account, we see *"Monitoring"* section on the left sidebar menu. We can turn monitoring on by pressing the blue button:



Everything works almost like a charm.

Extending basic setup

Monitoring data is stored in ES indexes and it is recommended to store those indexes on a separate ElasticSearch cluster. Well, if your cluster goes down and will not be able to start again, it may be great to

take a look at the monitoring data to figure what was going on, before the cluster crashed. Additionally, You may want to present monitoring dashboards without providing admin credentials.

All of these can be solved with Search Guard.

Exporting monitoring data to another cluster

X-Pack monitoring agents are used to capture diagnostics data and export them either locally or to another cluster. Moreover, it is possible to export data to a cluster secured by Search Guard.

In our demo we can setup another cluster on the same local machine running on a different port. This can be accomplished by the following entry in *elasticsearch.yml*:

```
http.port: 19200
```

Then, we need to configure X-Pack exporters:

```
xpack.monitoring.exporters:
  id1:
    type: http
    host: ["https://localhost:19200"]
    auth:
      username: admin
      password: admin
    ssl:
      certificate_authorities: root-ca.pem
```

We just need to specify cluster hosts, authentication parameters and a path to SSL certificate, which may be our root-ca.pem

Creating monitoring user

Let us now create a user with permissions dedicated to accessing monitoring data on a monitoring cluster. Search Guard comes with predefined roles:

- **sg_kibana_user** - this role has the minimal permissions required to use Kibana
- **sg_xp_monitoring** - this role has the required permissions to access monitoring in Kibana

Based on that, we can create a role mapping in *sg_roles_mapping.yml*:

```
sg_xp_monitoring:
  backendroles:
    - xp_monitoring

sg_kibana_user:
  backendroles:
    - kibanauser
```

and a user in *sg*internal*users.yml*:

```
screen_monitor:
  hash: $2y$12$MQjxoV607aDfVvJnKcVYqeGST3rOoGOazAhbVZTMQ548Ykr19YrCi
  roles:
    - kibanauser
    - xp_monitoring
```

where password hash has been generated by a hash.sh script from plugins/search-guard-6/tools directory. Running the script may require adding execute permissions on a file (chmod +x ../tools/hash.sh)

Do not forget to reload cluster config after that:

```
./sgadmin.sh -cd ../sgconfig/ -icl -nhnv  \
   -cacert ../../../config/root-ca.pem \
   -cert ../../../config/kirk.pem \
   -key ../../../config/kirk-key.pem
```

Enjoy the power of Search Guard and X-Pack Monitoring!

Where to go next:

- Read about Search Guard X-Pack support in our official documentation
- Browse all sample roles that Search Guard ships with
- If you have problems configuring TLS, read our TLS troubleshooting guide or ask for help on our forum.

Image: shutterstock / Graphic farm

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