sgctl - Take back control

Jochen Kressin · 2022-08-08

In this article, we look at the new Search Guard Control command line tool that ships with Search Guard FLX and demonstrate how easy it has become to configure security for Elasticsearch.

The Story so Far: sgadmin

Since the very first release for Elasticsearch 2, Search Guard shipped with a command line tool called sgadmin. You would use sgadmin to upload your security configuration to the cluster and to perform maintenance tasks. The tool hopefully served you well over the course of time, but with the arrival of Search Guard FLX, it was about time to rethink our approach to how security settings should be managed.

> TLS admin certificates are at the center of security configuration

TLS Admin Certificates

TLS admin certificates are at the center of the Search Guard security configuration. Whenever you want to make any changes, like changing a role or adding a user, you need to use a TLS admin certificate. Regular users are not allowed to change any security settings at all.

We made the deliberate decision to use TLS certificates instead of a simple root user with a username and password. From a security perspective, this provides a greater level of security. However, it also has some practical annoyances.

sgadmin Usage

Nearly all sgadmin calls require you to use a TLS admin certificate. This means that you have to specify the root CA, the Admin certificate and key, and information about your cluster location for every call. A typical call might look like this:

```
$ ./sgadmin.sh
   -cacert /path/to/root-ca.pem
   -cert /path/to/admin-cert.pem
   -key /path/to/admin-cert-private-key.pem
   -h elasticsearch.example.com
   -cn mycluster
   <actual command>
```

> Meet sgctl, our new shiny administration tool for Search Guard FLX.

If you work with sgadmin a lot, this can become a bit annoying. If, for example, you want to move some configuration from staging to production, you need to remember all these settings for both systems.

Meet sgctl, our new shiny administration tool for Search Guard FLX.

sgctl: Connection Profiles

With sgctl, we took a different approach and separated the connection settings from the actual commands you want to execute.

When you first connect to your cluster, you still need to provide the TLS certificates as before. Note the explicit *connect* command: sgctl will store the connection settings for this host in the .searchguard directory inside your home directory.

```
$ ./sgctl.sh connect elasticsearch.prod.example.com
  --ca-cart /path/to/prod-root-ca.pem
  --cert /path/to/prod-admin-cert.pem
  --key /path/to/prod-admin-cert-private-key.pem
```

So the next time you want to connect with your cluster, you just need to type:

```
$ ./sgctl.sh connect elasticsearch.prod.example.com
```

Any subsequent command will automatically use this connection profile. No need to specify all the connection details anymore. Say you want to fetch the current security configuration of your connected cluster, you just need to:

```
$ ./sgctl.sh get-config -o sg-config
```

Where -o specifies the output directory. Likewise, adding a new user to the internal user database is now as simple as:

```
$ /sgctl.sh add-user userName --password
```

This allows you to manage different connection profiles, e.g. one for staging and one for production.

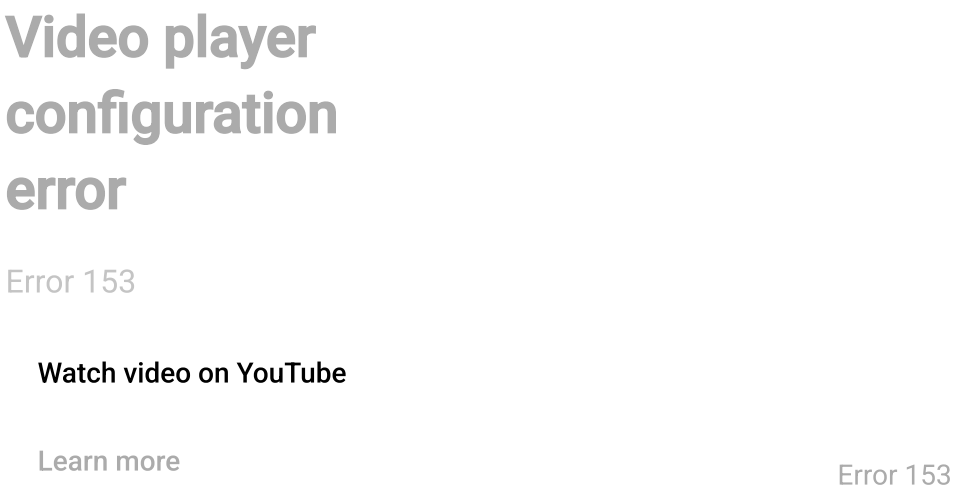
Moving Security Configuration From Staging to Production

Let's say you worked on your security configuration on your staging system. You tested everything and now it's time to move to production.

This can now be accomplished by these four simple commands:

```
$ ./sgctl.sh connect elasticsearch.staging.example.com
$ ./sgctl.sh get-config -o sg-config
$ ./sgctl.sh connect elasticsearch.prod.example.com
$ ./sgctl.sh update-config sg-config --force
```

The configuration will be pushed to your production system and changes take effect immediately. Pretty cool, isn't it?



What's More?

We will be adding more features to sgctl in the next releases. But we already have some more under our belt:

- Manage configuration variables so your config files can stay secret-less
- Migrate SG7 style configuration files to the new FLX formar
- Get information about the Search Guard version, components states and license information
- Change single properties of the security configuration directly without the need to upload complete configuration files

Where to go Next

- Head over to our docs to learn more about Search Guard FLX
- Try out FLX by downloading and running our demo installer

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