Changing Elasticsearch TLS certificates at runtime

Jochen Kressin · 2020-07-27

Search Guard secures your Elasticsearch cluster and the Elastic Stack by making heavy use of TLS certificates. This makes sure your traffic is safe against man-in-the-middle attacks and that only trusted nodes can join your cluster. But what if your certificates are about to expire and you need to exchange them?

Up until now, this required a multi-step process, including rolling restarts of your nodes. Since Search Guard v43, we support certificate hot reloading, making it easier than ever to manage the certificates you use for Elasticsearch. Combine that with certificate revocation lists, which we covered in the last post you have all the tools you need for easy TLS certificate management.

What's the reason for changing certificates?

There are several cases when you want to exchange your TLS certificates. The first one is also the most obvious - they are about to expire: In most cases, the certificates you or your PKI generates will have an expiration date. In fact, most modern browsers even reject certificates that have a very long expiration date. These can be certificates you use on the transport layer (traffic between nodes) or the REST layer.

> Certificate reloading in combination with certificate revocation lists gives you all the tool for easy certificate management

And while probably not the most usual use case, there also might be a situation where you want to replace intermediate CAs, or even the root CAs. Possibly an intermediate certificate has been compromised and was being revoked. Or, the private key of your root CA has been leaked, rendering all certificates signed with this CA invalid.

Luckily, Search Guars supports hot-reloading of any type of certificate on a running cluster.

How to change certificates - until now

Until now, Search Guard would load TLS certificates only when a node starts. Once the certificates had been loaded and verified, there was no way of changing them at runtime.

If you needed to change, say, a node certificate, the only way to do that was to install the new certificate on your node, and then restart this node.

Changing intermediate or root CAs was even more painful: You first had to add the new root CA to all nodes and the current one. Then perform a rolling restart. After that was done, remove the now un-used root CA, and perform a rolling restart again. Especially for large clusters, this was a lengthy process and nothing you want to do too often on a production system.

Luckily, you can now reload certificates at runtime, doing away with any node restart or rolling restart.

Certificate hot-reloading

Let's look at how certificate hot-reloading simplifies this whole process.

Let's say one or more leaf certificates are about to expire. That could be node certificates or REST layer certificates.

In the simplest case, just replace the certificate files, using the same file name as before, on any node. Then, call the new certificate reload REST API.

For transport (node-to-node) certificates, use:

```
POST /_searchguard/api/ssl/transport/reloadcerts/
```

For REST layer certificates, use:

```
POST /_searchguard/api/ssl/http/reloadcerts/
```

Calls to this API requires you to use a TLS admin certificate for authentication. You also need to call this API endpoint on any node in your cluster where you want to reload the certificates. There is no single command to reload them on all nodes at the same time.

Why is there no cluster-wide reload command?

Because TLS certificates are at the heart and core of Search Guard, any error here could break communication between nodes. Leaving you with a split or even non-functional cluster. So the safest approach is to exchange and reload the certificates one by one. Of course, reloading certificates can be scripted or executed by a tool like Puppet. Making the reload command node-specific should strive for the right balance between convenience and safety.

However, we would love to hear your opinion on that! Do you agree? Or would you still like to see a cluster-wide reload command? Let us know on our Search Guard Forum!

Exchanging root CAs

Exchanging root CAs on a running cluster is also possible, but this requires some additional steps. We will cover changing root CAs in our next part of this article series.

Where to go next

- Read the next article in this series about how to reload root CAs
- Read the full documentation on TLS hot reload
- Read about certificate revocation lists for another tool in your TLS management belt
- Satisfied with this new feature? Have some additional requirements or ideas? Drop us a note on our forum or contact us directly

Image: shutterstock / DestroLove

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