Search Guard puts security first

Jochen Kressin · 2018-01-30

Let's face it: security is not an easy topic. Implementing security correctly is quite hard. There are a plethora of attack vectors you need to consider. You need to keep track of newly discovered exploits, know the ins and outs of certificates and PKI infrastructures, and make sure your data is secure when accessed from internal or external networks. At Search Guard, we are very opinionated about this topic. We have and always will put "Security First".

When designing Search Guard, we had to make a lot of decisions regarding the general security architecture. In many cases, this meant to strive a balance between ease-of-use and to provide the highest level of security possible. Every time we had to make these kinds of decisions our approach was clear: We put security first, even if it meant sacrificing ease-of-use. Your data is too sensitive and too valuable to take any shortcuts.

And we could have taken many shortcuts too when implementing Search Guard, and make it a "one-click-security-solution". But we did not. We wanted to make it mandatory for Search Guard users to familiarize themselves with essential security technologies like encryption, TLS, certificates and PKI infrastructures.

> There is no such thing as one-click security. If you want to protect your data, you have to familiarize yourself at least with essential security technologies and terminologies. Any solution that claims to provide easy out-of-the-box security in fact only offers fake security.

We never had default users or passwords

One of the most important decisions was not to install any default users and password when you set up Search Guard. After the initial installation, Search Guard is like a blank canvas, and you need to actively make yourself familiar with the Search Guard authentication flow to plan and implement your security strategy. Not having any default users and passwords was always a cornerstone of Search Guard, and it seems that others are slowly adopting this view as well. As we all know, default passwords never get changed.

One question remains: How can you configure Search Guard if there is no built-in admin user? To solve this chicken and egg problem we again relied on TLS: In order to set up users, roles and permissions, you need to create and use an admin certificate. This certificate will then give you access to view and modify the Search Guard security configuration. This means:

- All aspects of this certificate are managed by you
- The certificate and its password is 100% under your control
- The certificate is validated against your PKI
- The certificate can be revoked by using a Certificate Revocation List

Does this make the usage of Search Guard easier? Probably not. Does it make Search Guard more secure? Definitely yes.

TLS on transport layer was always mandatory

Another very important decision was to make TLS mandatory on the Transport Layer and had this feature right from the very first release. Search Guard will refuse to start if you don't configure TLS properly. This means that you have to deal with certificates, ciphers and trust chains.

However, TLS on transport layer is a very important building block in your Elasticsearch security infrastructure. Without it, anyone can connect with a Transport Client and gain full access to your data. Or someone just sniffs the inter-node traffic. Or fires up a node and let it join your cluster. A lot of attack vectors that are easy to exploit. So setting up a proxy or providing security on REST only is not enough. We strongly contradict the claim that transport TLS does not add any security.

We received many requests over time to make TLS on transport optional. Partly because users did not want to have to deal with TLS, partly because of performance concerns. However, we politely declined those requests for one reason:

> If the inter-node traffic is not secured by TLS, any other security measure is in vain. Your cluster is open and data can be sniffed and tampered with easily.

Networks can't be trusted

"My servers are inside a VPN, we have firewalls and all that. Our internal network is safe, I don't need TLS" is something we often hear. Be aware that nowadays most attacks come from inside your network, not from the outside. And it does not need to be a malicious employee with bad intents. What about your

freelancers, contractors or business partners connecting to your network? What about accidental misconfiguration of your firewalls or proxies?

That's why we decided to make TLS mandatory. Security First means that we first worry about the safety of your data and that usability comes second. And it seems others have finally adopted our view as well.

Taking care of all the details

Getting basic security right is a first step, but it does not end there. While we firmly believe that using TLS everywhere is the best technique to secure your data as of today, TLS itself can also have flaws. While Heartbleed was a very prominent example, there are more, often suttle things to consider. For example, which exact TLS versions do allow? Which ciphers do you use? What about HTTPS compression?

We closely monitor the security landscape and provide sensible, secure settings for Search Guard, like:

- The vulnerable and outdated TLSv1 is disabled by default
- Client-side TLS renegotiation is disabled by default
- HTTPS compression is disabled by default
- You can configure which TLS versions are allowed and which not
- You can configure which cipher suites are allowed and which not

Open Source makes security audits possible for everyone

Our standpoint here is clear: Security means Open Source by definition. While Search Guard is dual licensed it was never an option for us to release the commercial modules as Closed Source Software. In other words – all of our code is available on GitHub. You can download, analyze and inspect every part of Search Guard.

This might seem like a risky move from a business perspective, but since we take the Security First approach serious, it was always clear this is something we have to do. If you buy a security solution from a vendor and you are not able to inspect the code, you're left with only one option: Trust the vendor. Trust that the software does what the vendor claims it does. Trust that the code has no hidden backdoors or vulnerabilities. Trust that then vendor fixes bugs and security issues in time.

Our code has been inspected and audited many, many times. By us, by the Open Source community, and by security experts and auditors from our customers. This already provides a high level of trust, and if you want, you can also run audits of your own.

Can you be sure your security vendor correctly deals with clearing in-memory passwords when authenticating users? Can you be sure your vendor protects against Active Directory / LDAP timing attacks when authenticating users? With Search Guard, you can!

Summary

Search Guard always followed the Security First approach. This mantra drives many of our technical and business decisions, and it is our highest priority to provide you with the best security solution for

Elasticsearch. By making all of our code Open Source you do not have to only trust our word, but can verify the integrity and security of our code yourself.

Where to go next

- Read about how to setup and configure TLS for Search Guard
- Read more about TLS for production environments
- If you run into any TLS issues, head over to our TLS Troubleshooting guide

---

This article was published on the Search Guard blog: https://search-guard.com/blog/search-guard-puts-security-first/