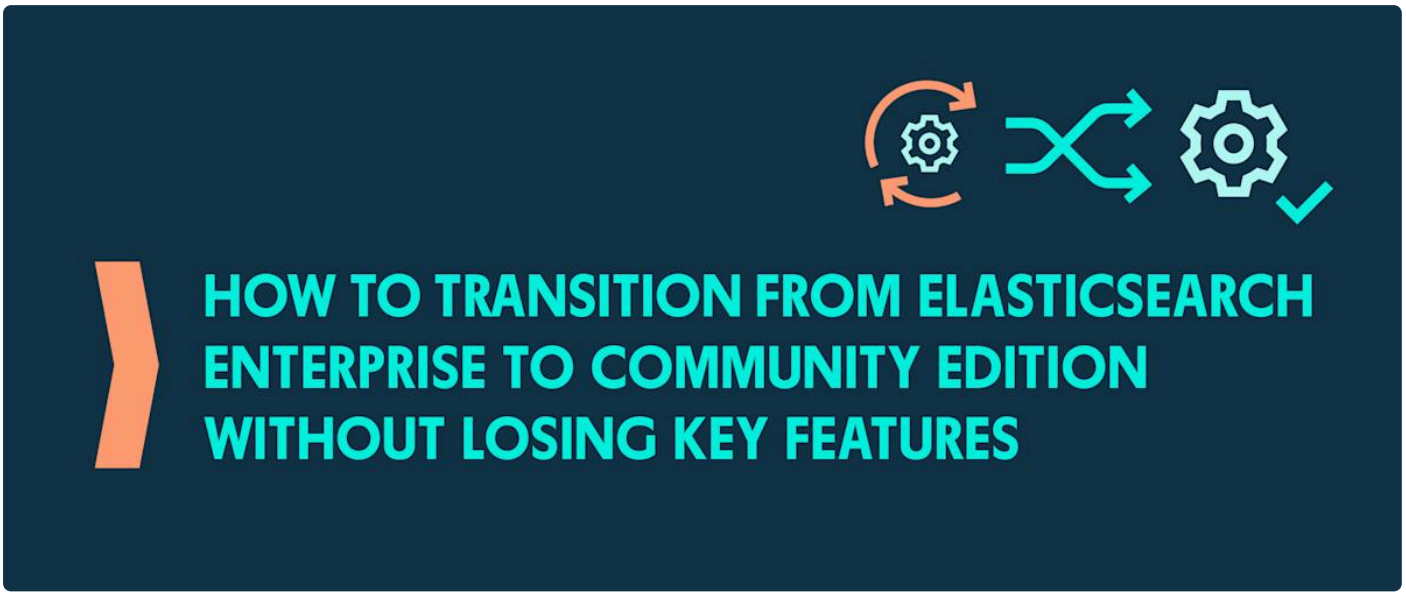
How to Transition from Elasticsearch Enterprise to SearchGuard Community Edition

Daniel Gleim · 2025-04-09



Migrating from Elasticsearch Enterprise to the Search Guard Community Edition is a smart choice for many organizations, especially for those looking to reduce costs without compromising on security features. While Elasticsearch Enterprise can be costly, the Search Guard Community Edition offers enterprise-grade security for free. This guide outlines the key steps involved in making the switch while preserving the security configurations and certificates from your existing Elasticsearch setup.

Why Make the Switch?

Cost Savings

One of the most immediate benefits of transitioning to Search Guard Community Edition is the significant reduction in licensing costs. Unlike Elasticsearch Enterprise, which requires expensive licenses based on deployment size, Search Guard Community Edition provides robust security capabilities at no cost.

Retaining Key Security Features

Search Guard Community Edition is not a watered-down version. It supports the core security features that are essential for protecting your Elasticsearch cluster:

1. Encryption (for both REST and transport layers)
2. Role-based access control (RBAC)
3. Authentication (including PKI and proxy authentication)
4. Alerting and Monitoring

By switching to Search Guard Community Edition, you can retain these crucial features without incurring any additional costs.

Step-by-Step Guide to Transition from Elasticsearch Enterprise to Search Guard Community Edition

Step 1: Disable Shard Allocation

Disable shard allocation to prevent Elasticsearch from attempting to redistribute shards. This can be done using either *sgctl* or *curl*.

1. Using sgctl

```
./sgctl.sh rest put _cluster/settings  \
    --json '{"persistent":{"cluster.routing.allocation.enable": "none"}}'
```

2. Using curl

```
curl -Ss -XPUT 'https://localhost:9200/_cluster/settings?pretty' \
-H 'Content-Type: application/json' -d'
{
  "persistent": {
    "cluster.routing.allocation.enable": "none"
  }
}'
```

Step 2: Stop Elasticsearch

Once shard allocation has been disabled, you can safely shut down the Elasticsearch cluster. Depending on how Elasticsearch was started, use one of the following methods:

1. If you are running Elasticsearch with systemd:

```
sudo systemctl stop elasticsearch.service
```

2. If you are running Elasticsearch with SysV init:

```
sudo -i service elasticsearch stop
```

3. If you are running Elasticsearch as a daemon:

```
kill $(cat pid)
```

Step 3: Install Search Guard Plugin

More information about the installation can be found here.

Before configuring Search Guard, you must install the plugin on your Elasticsearch nodes. Note that the Search Guard version must match your Elasticsearch installation's exact version. For example, if you are running Elasticsearch 8.17.5, then you need to install Search Guard for this version. Example:

```
sudo bin/elasticsearch-plugin install \
    https://maven.search-guard.com/search-guard-flx-release/com/floragunn/search-guard-flx-
elasticsearch-plugin/3.0.3-es-8.17.5/search-guard-flx-elasticsearch-plugin-3.0.3-es-8.17.5.zip
```

You can see a list of all available version on the Search Guard Version Matrix page.

Step 4: Prepare Certificates

Search Guard requires certificates to secure your Elasticsearch cluster. You'll need certificates for both the transport and REST layers. These certificates can either be generated using OpenSSL or through your existing PKI infrastructure.

Transport Layer: Ensures encrypted communication between Elasticsearch nodes. *REST Layer(Optional):* Enables HTTPS for the REST API layer if required.

Step 5: Add TLS Configuration

Once you have your certificates ready, you need to configure TLS (Transport Layer Security) for both the transport and REST layers. Here's how you can do it in your `elasticsearch.yml`

5.1 Transport Layer Encryption & Admin Certificate Configuration

This ensures secure communication between nodes by enabling TLS on the transport layer and specifying the admin certificate.

Add the following configuration to `elasticsearch.yml`

```
Search Guard.ssl.transport.pemcert_filepath: <path_to_node_certificate>
Search Guard.ssl.transport.pemkey_filepath: <path_to_node_certificate_key>
Search Guard.ssl.transport.pemtrustedcas_filepath: <path_to_root_ca>
Search Guard.ssl.transport.enforce_hostname_verification: true
Search Guard.ssl.transport.pemkey_password: <password>  # Optional, if your private key is
password-protected
Search Guard.authcz.admin_dn:
  - CN=kirk,OU=client,O=client,L=test,C=de
```

- *Search Guard.ssl.transport.pemcert_filepath:* Path to the node certificate.
- *Search Guard.ssl.transport.pemkey_filepath:* Path to the node certificate's private key.
- *Search Guard.ssl.transport.pemtrustedcas_filepath:* Path to the root certificate authority (CA) certificate.
- *Search Guard.ssl.transport.enforcehostnameverification:* Enforces hostname verification for added security.
- *Search Guard.ssl.transport.pemkey_password:* Password for the private key, if it's protected (optional).
- *Search Guard.authcz.admin_dn:* Distinguished name (DN) for the admin certificate, used to configure and manage Search Guard.

5.2 REST Layer Encryption (Optional)

If you want to enable HTTPS for the REST API, you'll need to configure the TLS settings for the HTTP layer. Add this to `elasticsearch.yml`

```
Search Guard.ssl.http.enabled: true
Search Guard.ssl.http.pemcert_filepath: <path_to_http_certificate>
Search Guard.ssl.http.pemkey_filepath: <path_to_http_certificate_key>
Search Guard.ssl.http.pemtrustedcas_filepath: <path_to_http_root_ca>
```

Step 6: Restart Elasticsearch Nodes

After configuring the certificates and the TLS settings, restart all Elasticsearch nodes to apply the changes. Ensure that every node has the correct certificate configuration.

Step 7: Re-enable Shard Allocation

Once the cluster has restarted, re-enable shard allocation to allow Elasticsearch to distribute the data across nodes. Use the following command to re-enable shard allocation:

```
./sgctl.sh rest put _cluster/settings \
    --json '{"persistent":{"cluster.routing.allocation.enable": "all"}}'
```

Transferring Elasticsearch Configurations to Search Guard Community Edition

In addition to setting up TLS and certificates, you'll also need to transfer your existing configurations from Elasticsearch to Search Guard. This includes:

1. Roles and Permissions:

If you were using role-based access control (RBAC) in Elasticsearch Enterprise, you will need to migrate these settings to Search Guard. You can use Search Guard's `sgctl` tool to upload your role definitions, user permissions, and other configurations.

2. Users and Authentication Methods:

You can configure Search Guard to use the same authentication methods you had in Elasticsearch Enterprise, such as PKI-based authentication or proxy authentication. These settings should be replicated in the Search Guard configuration.

3. Search Guard Index Initialization:

The first time you use Search Guard, you'll need to initialize the Search Guard index by using the `sgctl` tool. This step is crucial for setting up the user authentication and authorization system:

```
./sgctl.sh rest put _cluster/settings \
    --json '{"persistent":{"cluster.routing.allocation.enable": "none"}}'
```

Once the Search Guard index is initialized, you can manage your roles, permissions, and authentication methods using the Search Guard configuration GUI or through `sgctl`.

Final Thoughts

Migrating from Elasticsearch Enterprise to Search Guard Community Edition provides several benefits, including significant cost savings and continued access to essential security features. By carefully transferring your certificates, configurations, and user settings to Search Guard, you can ensure a smooth transition without compromising on security.

Search Guard's Community Edition provides enterprise-grade protection, robust authentication mechanisms, and a flexible configuration system—all at no cost. With proper planning and execution, your migration will be straightforward and allow you to continue managing your Elasticsearch cluster securely.

For more information on configuring Search Guard or transitioning from Elasticsearch, refer to the official Search Guard documentation or reach out for additional support.

This article was published on the Search Guard blog: https://search-guard.com/blog/how-to-transition-from-elasticsearch-enterprise-to-searchguard-community/