SEARCH GUARD

ARCHITECTURE & REQUEST FLOW

Search Guard

01.

SEARCH GUARD TLS

- **Search Guard uses TLS on transport and REST layer**

→ Data encryption: No one can spy on your data

→ Data integrity: No one can alter your data

→ Cluster integrity: Only trusted nodes can join the cluster

- **TLS on transport layer:**

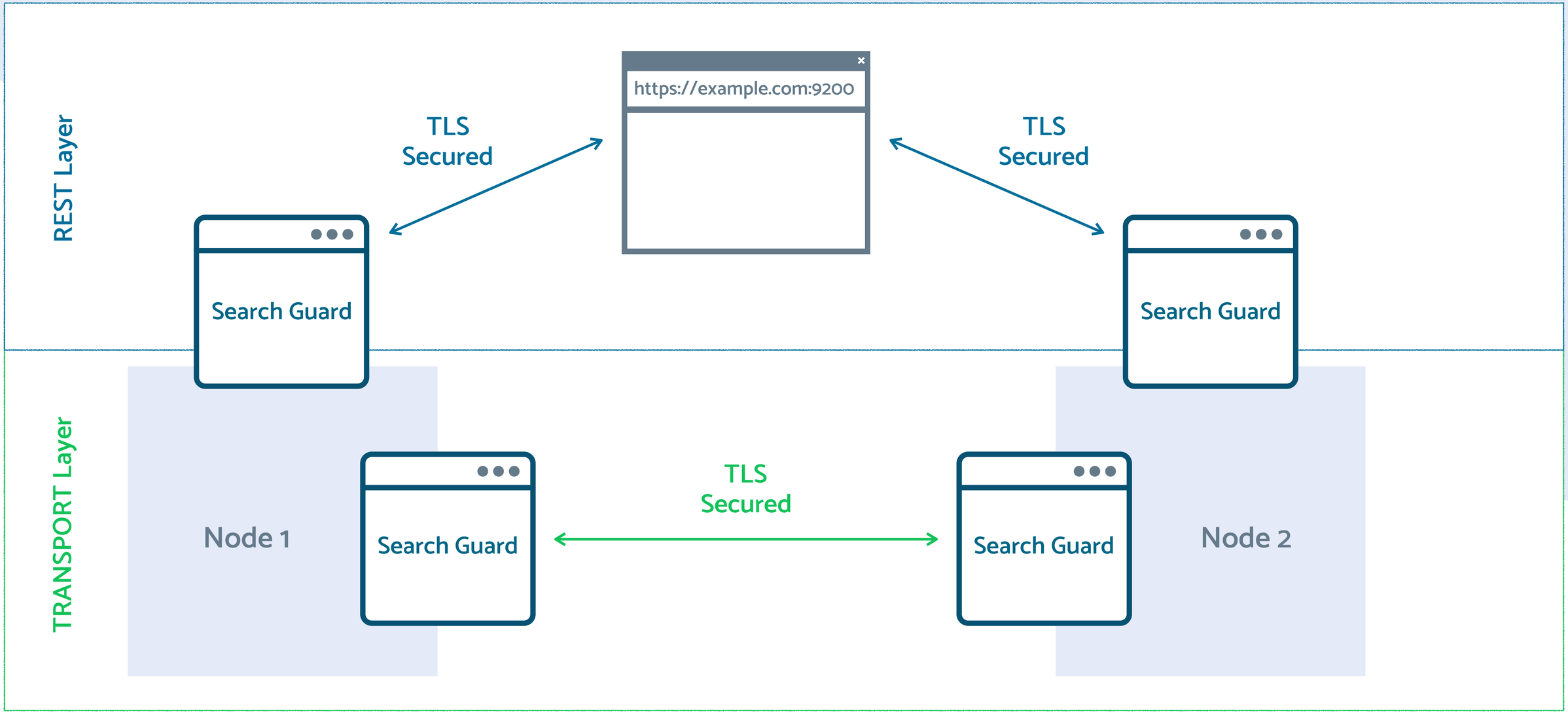
→ Protects data traveling between the nodes

→ Mandatory, cannot be switched off

- **TLS on REST layer:**

→ Adds HTTPS support

ENCRYPTION IN TRANSIT



02.

TLS CERTIFICATES

- **Search Guard uses three types of certificates**
- **Node certificates**

→ Used for inter-node traffic

→ Only nodes with a valid certificate can join the cluster

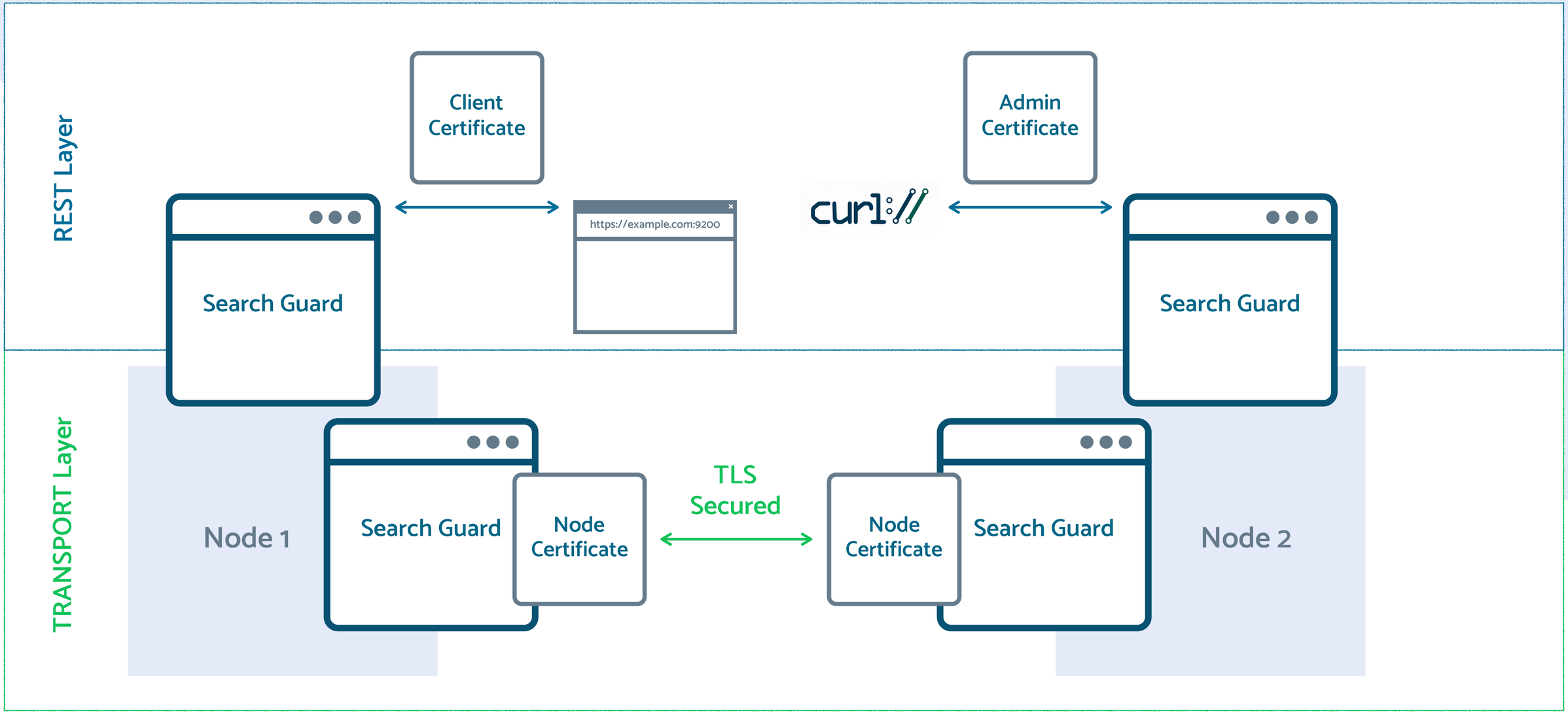
- **Admin certificates**

→ Grant root access to the cluster

- **Client certificates**

→ Can be used for client authentication and authorization

TLS CERTIFICATES



03.

SEARCH GUARD REQUEST FLOW

- **Applies to REST and transport layer likewise**
- **TLS certificate validation**

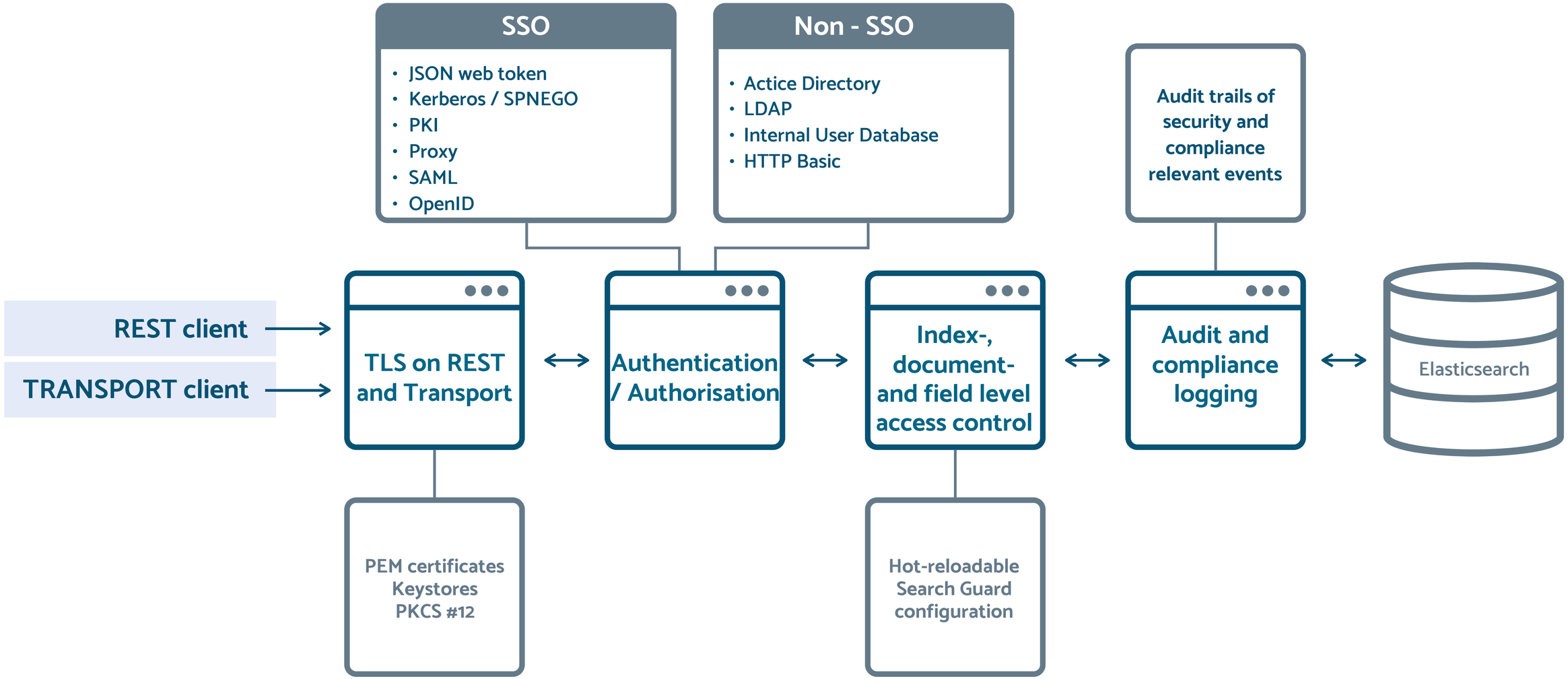
→ E.g., for transport traffic, validate the certificate of the peer node

- **Extract and verify user credentials**

→ Depends on the configured authentication domains

- **Assign Search Guard roles and evaluate permissions**
- **Apply index-, document- and field-level access control**
- **Apply audit and compliance logging**
- **Execute the request in Elasticsearch**

SEARCH GUARD REQUEST FLOW



04.

SEARCH GUARD AUTHENTICATION FLOW

- **Extract user credentials from request**

→ E.g., HTTP Basic, JSON web token, Kerberos ticket

- **Validate provided credentials**

→ E.g., LDAP authentication, JWT signature checks

- **Fetch backend roles for the authenticated user**

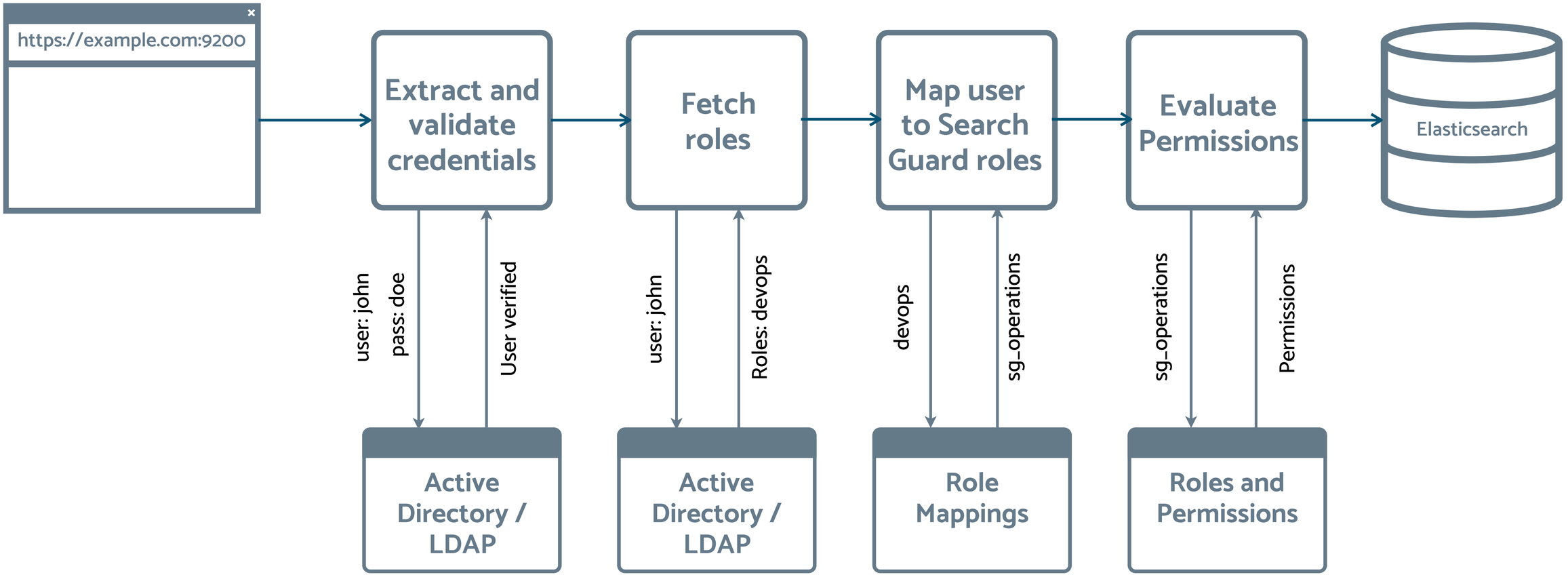
→ E.g., LDAP groups, JWT claims, SAML assertions

- **Map user to Search Guard role(s)**

→ Using username, backend roles or hosts

- **Evaluate the permissions assigned to the roles**

AUTHENTICATION FLOW

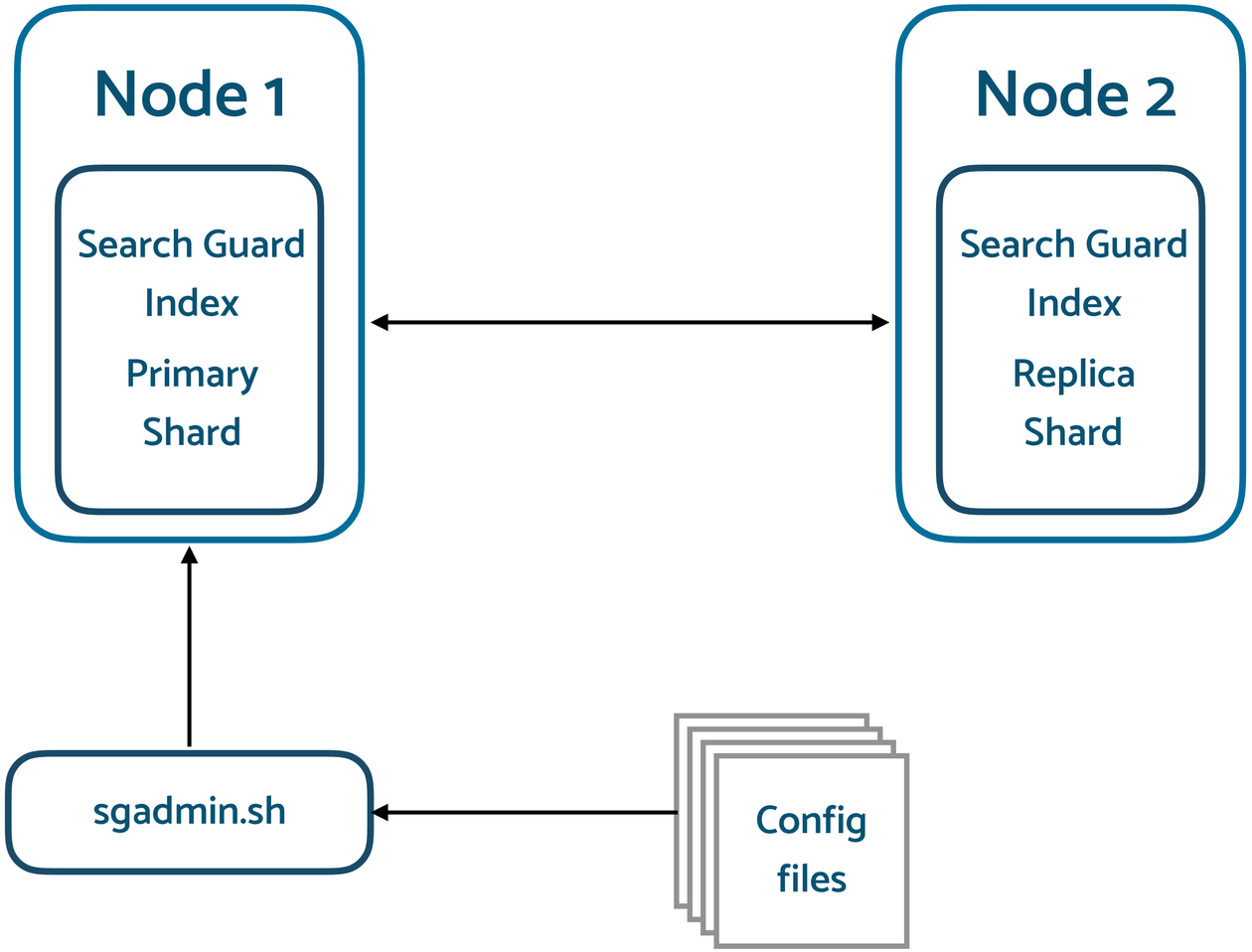


05.

SEARCH GUARD CONFIGURATION INDEX

- **Search Guard configuration is stored in an Elasticsearch index**
  - → Hot-reloadable
  - → Changes take effect immediately
  - → No configuration files necessary on nodes
- **Accessible only with TLS admin certificate**
- **Configuration changes can be applied by**
  - → sgadmin command line tool
  - → REST API
  - → Kibana configuration GUI

SEARCH GUARD CONFIGURATION INDEX



06.

RESOURCES

- **Search Guard website**

→ https://search-guard.com/

- **Documentation**

→ https://docs.search-guard.com

- **Community Forum**

→ https://groups.google.com/d/forum/search-guard

- **GitHub**

→ https://github.com/floragunncom

SEARCH GUARD SEND US A MESSAGE:

info@search-guard.com

Search Guard

floragunn GmbH
Tempelhofer Ufer 16
D-10963 Berlin, Germany

E-Mail: info@search-guard.com
Web: search-guard.com

Managing Directors: Claudia Kressin, Jochen Kressin
Registergericht: Amtsgericht Charlottenburg
Registernummer: HRB 147010 B
E-Mail: info@floragunn.com