SEARCH GUARD

QUICKSTART AND FIRST STEPS

Search Guard

01.

PLUGIN INSTALLATION

- **Find the matching Search Guard version for your Elasticsearch version**

→ https://docs.search-guard.com/latest/search-guard-versions

- **Use the Elasticsearch plugin command to install**

→ ./bin/elasticsearch-plugin install com.floragunn:search-guard-6:6.4.0-23.0

→ Confirm when being asked for plugin permissions

- **Alternative: Offline installation**

→ Download the plugin zip file

→ Use the offline install command

→ ./bin/elasticsearch-plugin install -b file:///path/to/search-guard-6-<version>.zip

02.

DEMO INSTALLER

- **Search Guard ships with a demo installer**

→ Set up a PoC in minutes

- **The installer will**

→ add demo TLS certificates for data encryption

→ add the TLS configuration to the elasticsearch.yml file.

→ initialize Search Guard with demo users and roles

→ generate a sgadmin_demo.sh script that you can use for configuration changes

03.

EXECUTING THE DEMO INSTALLER

- **Change to the tools directory of Search Guard**

→ cd ./plugins/search-guard-6/tools

- **Grant execution permissions to the installer and execute**

→ chmod 755 ./install_demo_configuration.sh

→ ./install_demo_configuration.sh

- **When prompted by the installer, answer as follows**

→ Install demo certificates? [y/N] y

→ Initialize Search Guard? [y/N] y

→ Enable cluster mode? [y/N] n

04.

TESTING THE INSTALLATION

- **Start Elasticsearch**

→ ./bin/elasticsearch

- **Test HTTPS encryption**

→ Use a browser and open https://localhost:9200/_searchguard/authinfo?pretty

→ Accept the warning message regarding self-signed demo certificates

- **Test admin log in**

→ When prompted, log in with admin/admin

→ Search Guard displays information about the logged in admin user

05.

ADDING KIBANA

- **Copy the download link for the Search Guard Kibana plugin**

→ https://docs.search-guard.com/latest/search-guard-versions

- **Install the plugin**

→ bin/kibana-plugin install https://url/to/search-guard-kibana-plugin-<version>.zip

- **Alternative: Offline installation**

→ Download the Search Guard Kibana plugin

→ bin/kibana-plugin install file:///path/to/search-guard-kibana-plugin-<version>.zip.

- **Wait for Kibana optimizer to finish**

→ Kibana requires this step, you cannot skip it

06.

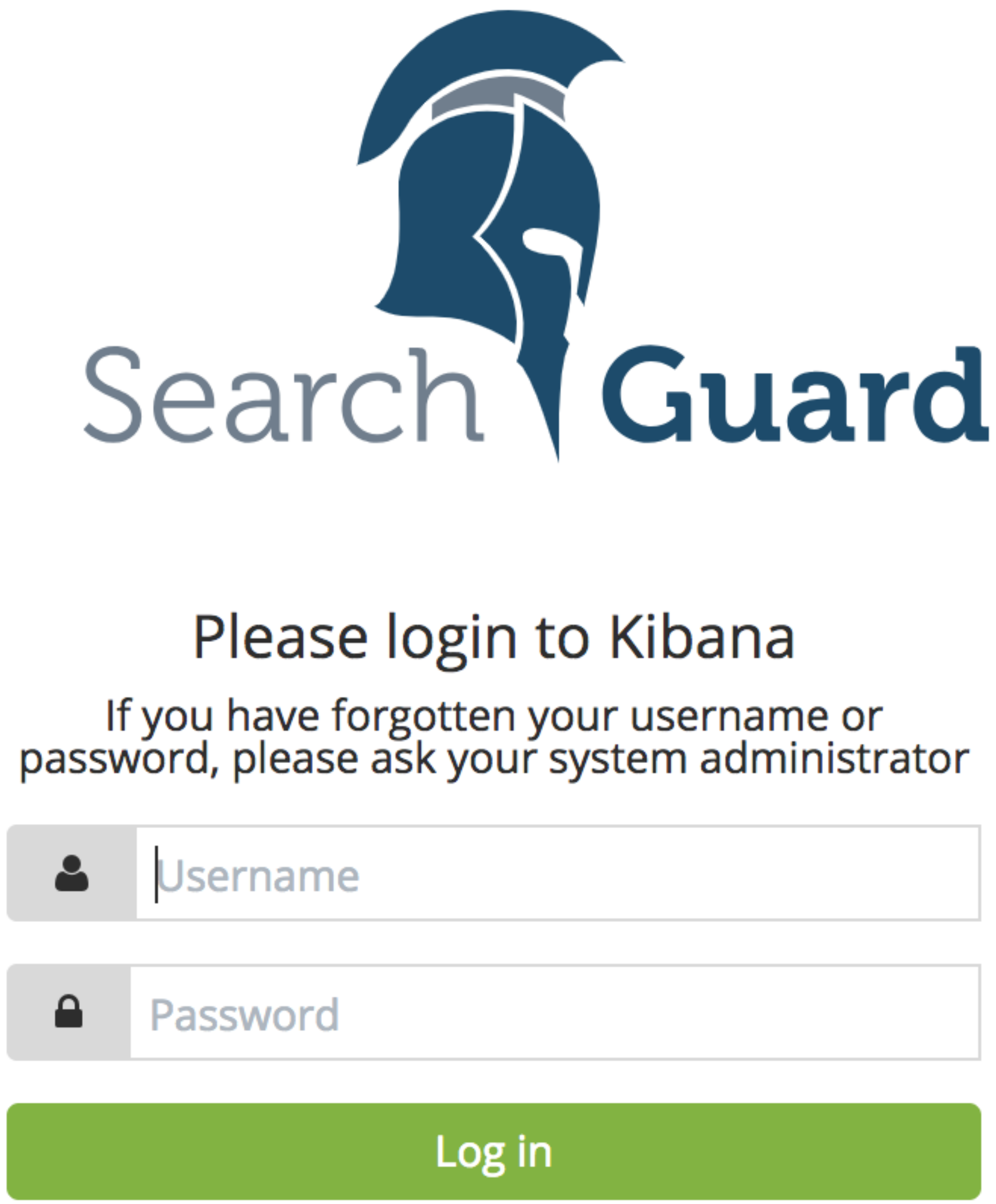
KIBANA MINIMAL CONFIGURATION

- Add the following configuration to kibana.yml

```
xpack.security.enabled: false
searchguard.auth.type: "basicauth"
elasticsearch.url: "https://localhost:9200"
elasticsearch.ssl.verificationMode: none
elasticsearch.username: "kibanaserver"
elasticsearch.password: "kibanaserver"
```

- Start Kibana
- Use a browser and visit http://localhost:5601/
- The Search Guard login page is displayed
- Use admin/admin to log in

SEARCH GUARD LOGIN PAGE



Please login to Kibana

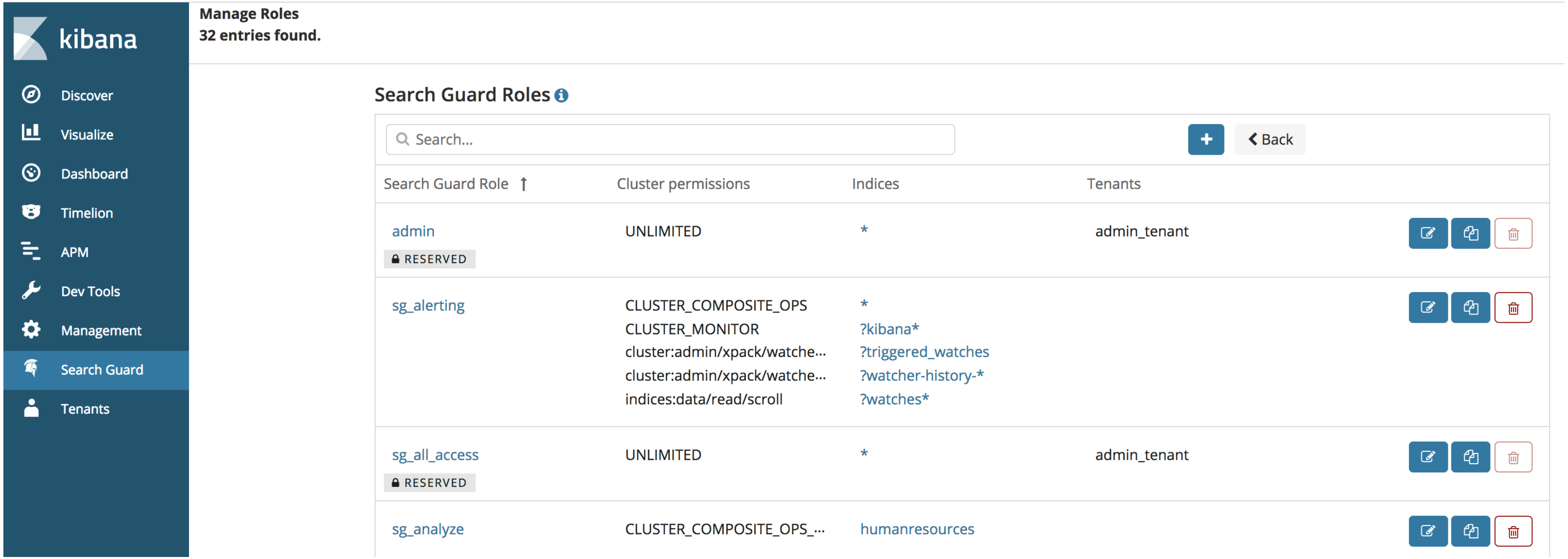
If you have forgotten your username or password, please ask your system administrator

07.

SEARCH GUARD CONFIGURATION GUI

- **Search Guard can be configured in three ways**
  - → Using the sgadmin command line tool
  - → Using the REST API
  - → Using the Kibana Configuration GUI
- **GUI can be used to configure**
  - → Users
  - → Roles
  - → Permissions

SEARCH GUARD CONFIGURATION GUI



Manage Roles
32 entries found.

Search Guard Roles

Search Guard Role ↑	Cluster permissions	Indices	Tenants
admin RESERVED	UNLIMITED	*	admin_tenant
sg_alerting	CLUSTER_COMPOSITE_OPS CLUSTER_MONITOR cluster:admin/xpack/watche... cluster:admin/xpack/watche... indices:data/read/scroll	* ?kibana* ?triggered_watches ?watcher-history-* ?watches*	
sg_all_access RESERVED	UNLIMITED	*	admin_tenant
sg_analyze	CLUSTER_COMPOSITE_OPS_...	humanresources	

08.

ADDING A NEW KIBANA USER

- **To use Kibana, a user needs to have the sg_kibanauser role**

→ Defines minimal permissions to access Kibana

→ Installed by the demo installer

- **In addition, a user needs permissions to access one or more indices**

→ We will add a new role for that

→ We will give this role READ access to one index

09.

CONFIGURING A SEARCH GUARD ROLE

- **Navigate to “Search Guard Roles”**
- **Click on the plus sign and give the role a telling name**

→ e.g. “sg_mykibanarole”

- **Navigate to “Cluster Permissions”**

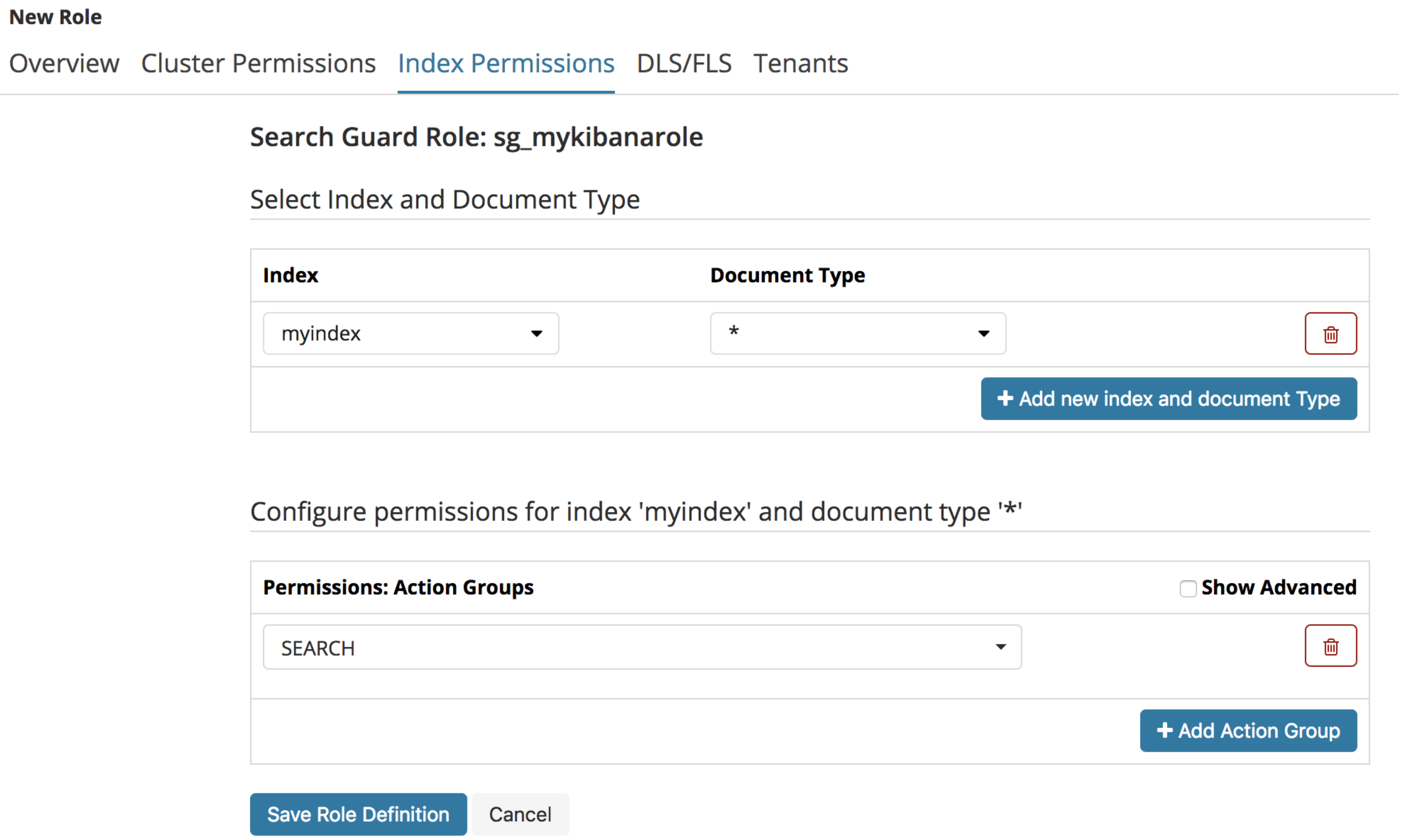
→ add the CLUSTER_COMPOSITE_OPS cluster permissions

- **Navigate to “Index Permissions”**

→ add a new index and use “*” as document type

→ add the SEARCH index permissions

ADDING A NEW SEARCH GUARD ROLE



Search Guard Role: sg_mykibanarole

Select Index and Document Type

Index	Document Type
myindex	*

Configure permissions for index 'myindex' and document type '*'

Permissions: Action Groups

SEARCH

10.

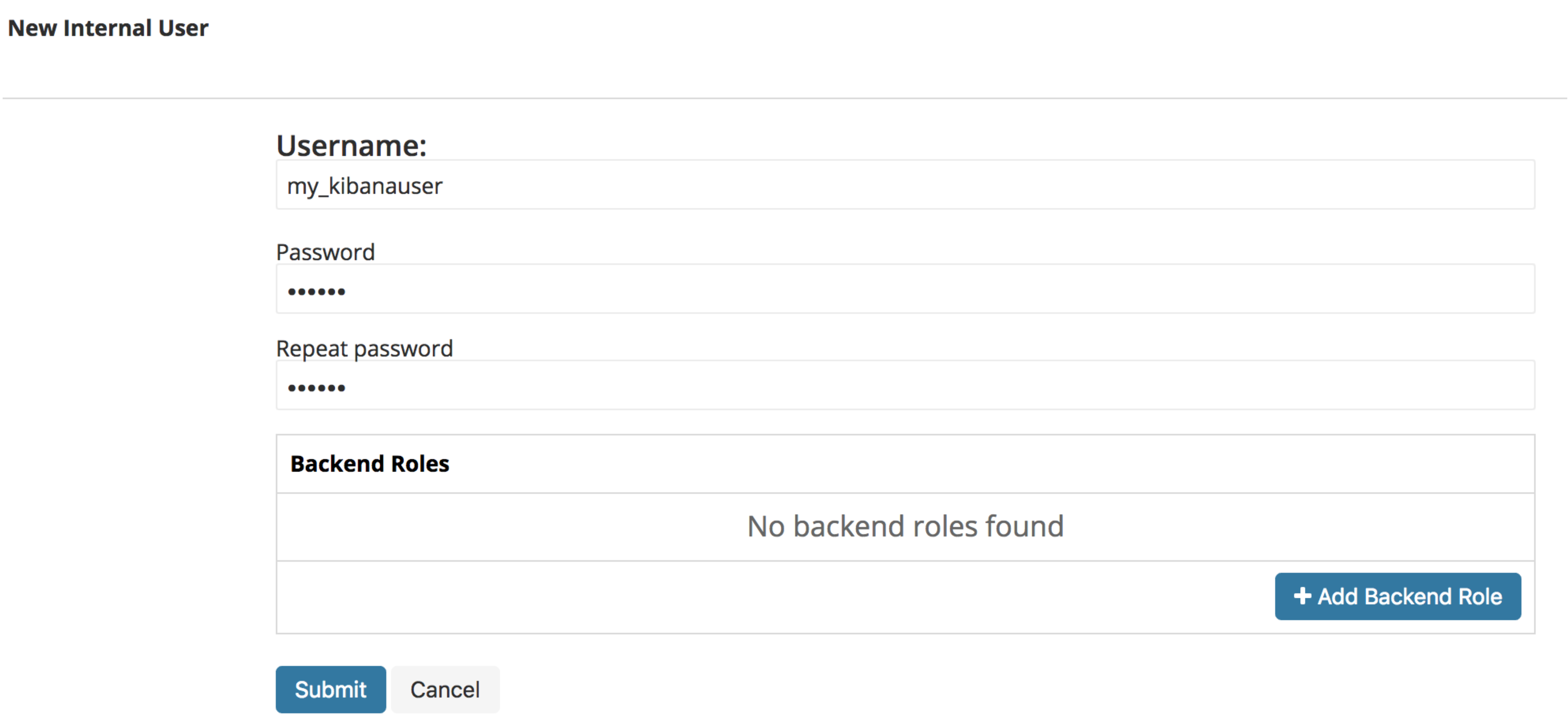
ADDING A NEW USER

- Navigate to “Internal User Database”
- Click on the plus sign and choose a username

→ e.g. “my_kibanauser”

- Choose a password
- Save the user

ADDING A NEW USER



New Internal User

Username:
my_kibanauser

Password
••••••

Repeat password
••••••

Backend Roles

No backend roles found

11.

MAPPING THE USER TO ROLES

- To assign Search Guard roles to a user, we use the role mapping
- Search Guard roles can be assigned by

→ username

→ backend roles

→ hostnames

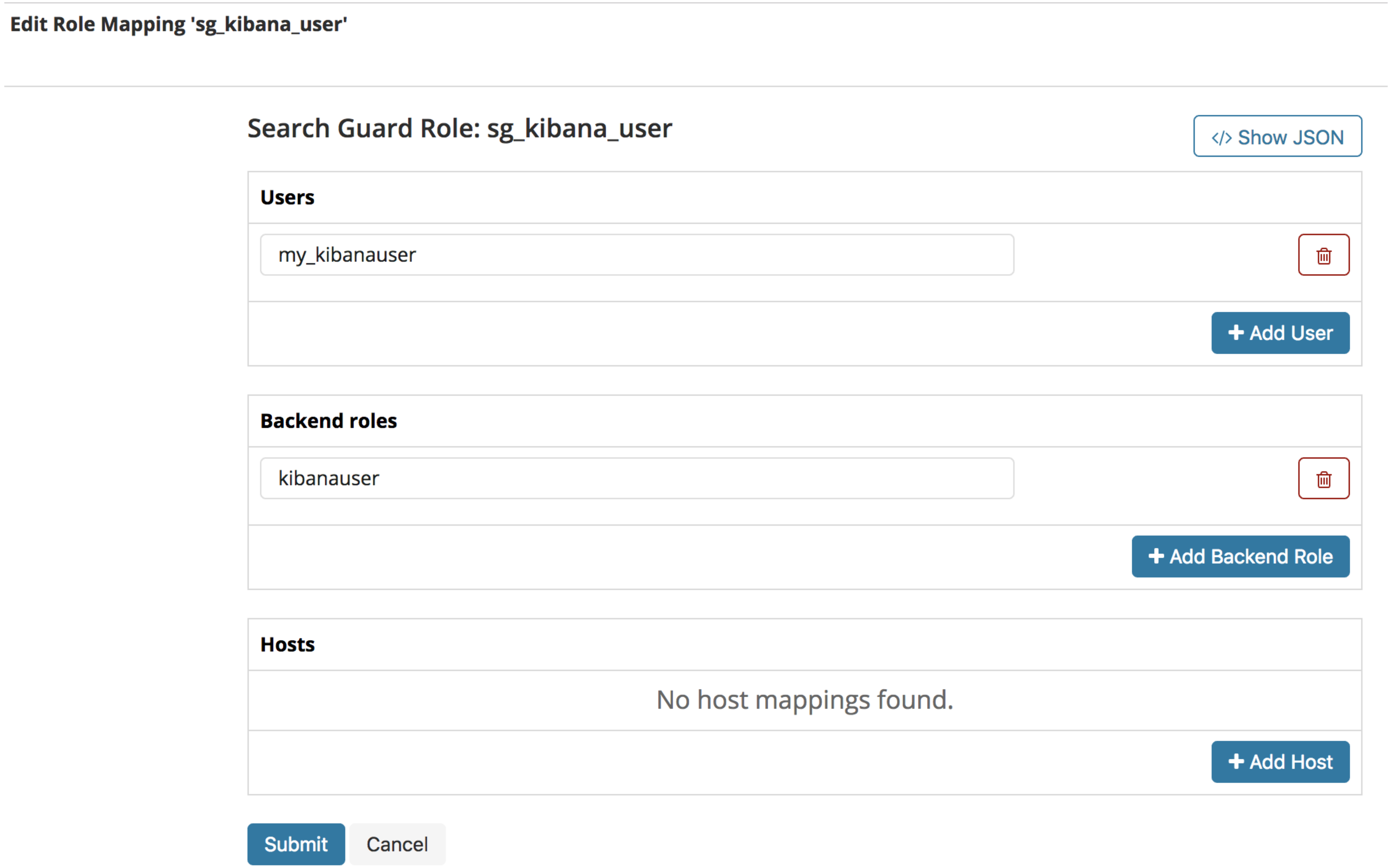
- We will add the user to the existing kibanauser mapping
- We will add a new mapping for our new Search Guard role

12.

ASSIGNING THE KIBANAUSER ROLE

- Click on “Role Mappings”
- Click on the “sg_kibana_user” mapping
- Add the “my_kibanauser” to the mapping

ASSIGNING THE KIBANAUSER ROLE



Edit Role Mapping 'sg_kibana_user'

Search Guard Role: sg_kibana_user

Users

my_kibanauser

Backend roles

kibanauser

Hosts

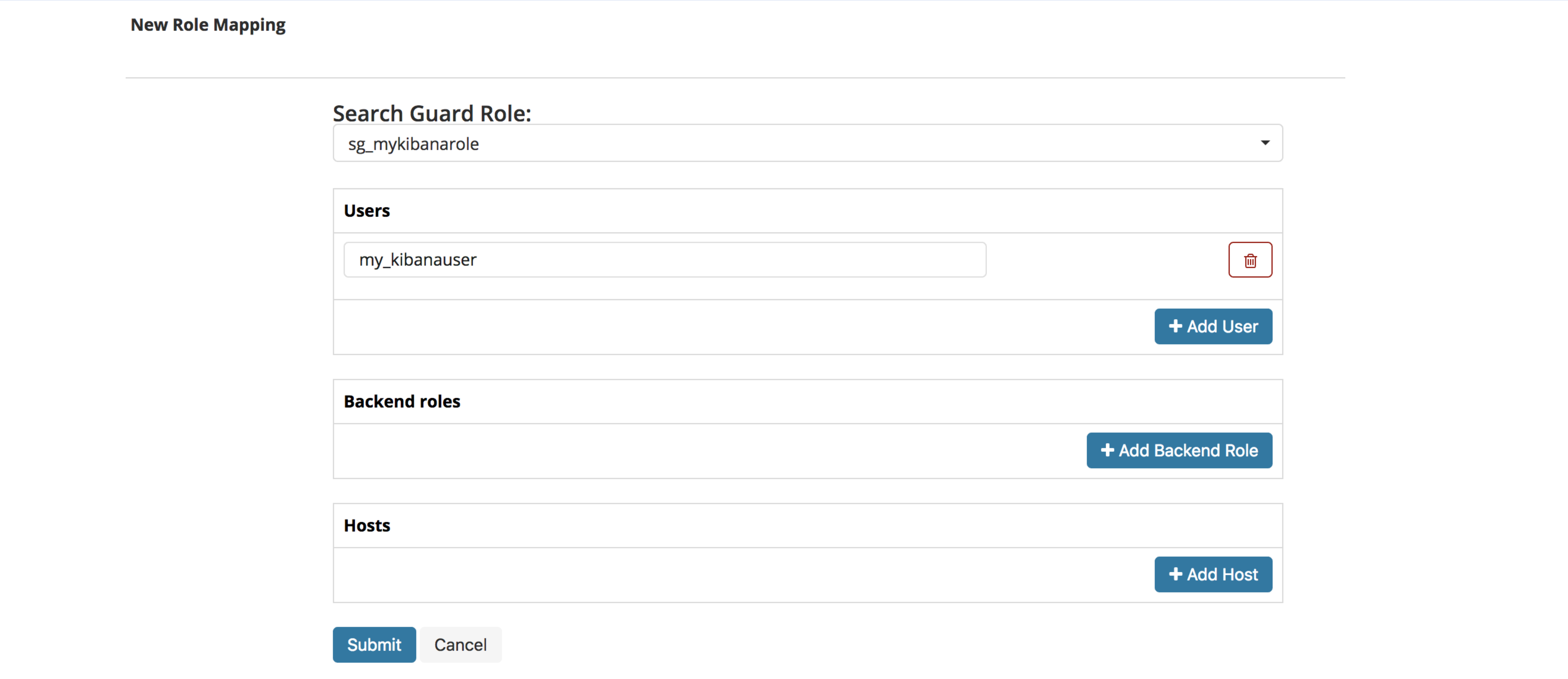
No host mappings found.

13.

CREATING A NEW MAPPING

- Click on “Role Mappings”
- Click on the plus sign
- From the drop-down, select the “sg_mykibanarole” role
- Add the “my_kibanauser” to the mapping

CREATING A NEW MAPPING



New Role Mapping

Search Guard Role: sg_mykibanarole

Users

my_kibanauser

Backend roles

Hosts

13.

TESTING THE NEW USER

- **Click on log out and log in with the new users**
- **Click on “Management” -> “Index Patterns”**
- **The new user should only see the “myindex” index**

→ This is the index we used when defining the sg_ mykibanarole

→ Of course, the “myindex” index has to exist …

14.

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/floraguncom

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

Search Guard