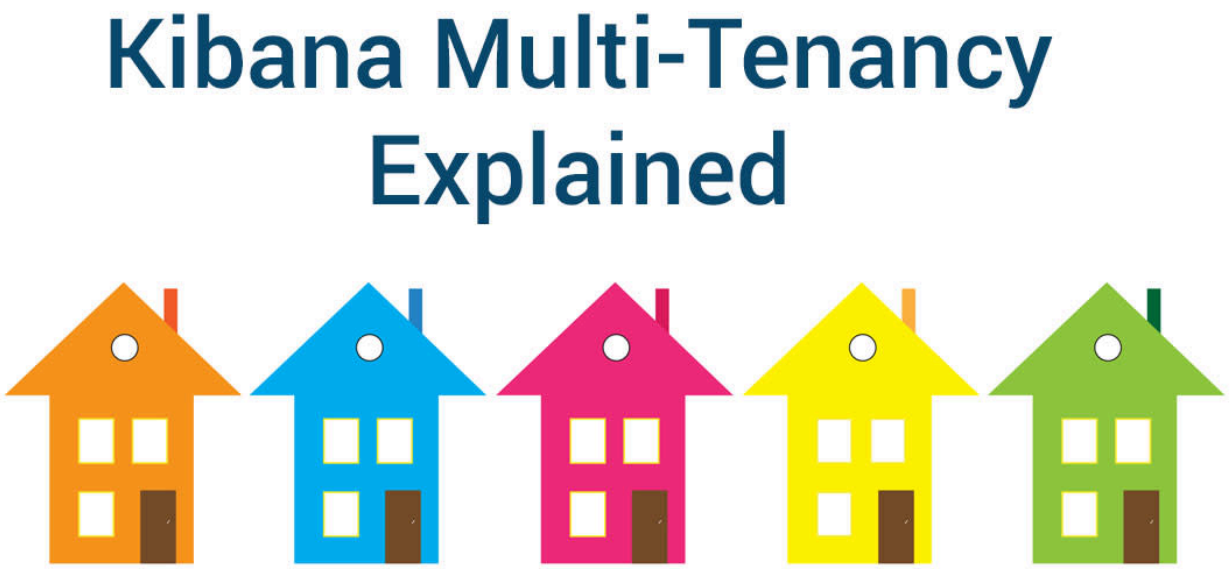
Kibana Multi-Tenancy Explained

Cliff Staley · 2020-11-24



Search Guard for Elasticsearch, and the Search Guard Kibana plugin work hand in hand.

On the Elasticsearch side, Search Guard governs access to any data stored in Elasticsearch. On the Kibana side, you can use the multi-tenancy feature to control who has access to Dashboards, Visualizations, and more.

How does Kibana organize data?

Elasticsearch organizes all data in *indices*. If you store a new document, you need to tell Elasticsearch to which index it belongs. If you query for documents, you need to specify against which index you want to run your query.

Kibana, on the other hand, does not have anything similar out of the box. Every Kibana object you save, like Dashboards, Visualizations, Stored Queries, will be kept in one *global* Elasticsearch index. By default, this index is called ".kibana".

In consequence, any Kibana user can see, modify, and delete objects created by other users.

What is Kibana Multi-Tenancy?

In Search Guard 5, we introduced the Multi-Tenancy feature for Kibana. Multi-Tenancy makes it possible to control access to Saved Objects based on Search Guard roles.

> A tenant is a named container for Saved Objects that provides access control based on Search Guard roles.

The easiest way to think about tenants is the Elasticsearch index analogy: Instead of storing everything in one global Saved Objects index, each tenant uses its own dedicated index. Search Guard then controls access to these tenant indices based on the roles and permissions a user has.

In other words: A tenant is a named container for Saved Objects that provides access control based on Search Guard roles.

Enabling Multi-Tenancy

First, make sure to enable Multi-Tenancy for Elasticsearch and Kibana:

sg_config.yml

```
sg_config:
  dynamic:
     multitenancy_enabled: true
     ...
```

kibana.yml:

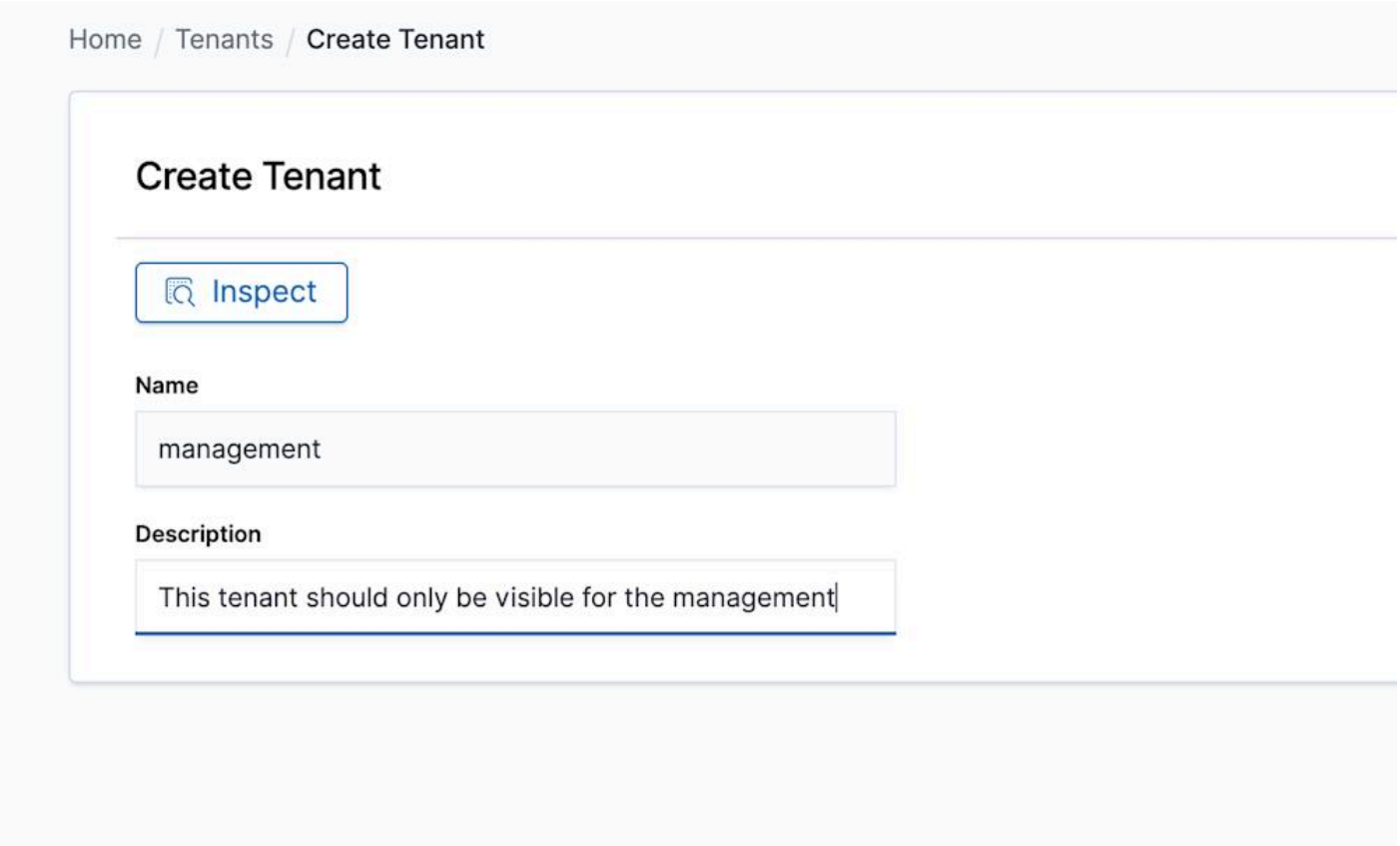
```
searchguard.multitenancy.enabled: true
elasticsearch.requestHeadersWhitelist: ["sgtenant", "Authorization"]
```

Adding tenants

You have three options for adding tenants to Kibana:

- Add tenants to sg_tenants.yml and use sgadmin to upload the changes
- Use the Multi-Tenancy REST API
- Use the Kibana Search Guard UI

In this post, we use the Kibana UI. Navigate to the Search Guard Configuration page, click on "Tenants," and then on "Create Tenant". Give your new tenant a name and an optional description, and save it.



Assigning tenants to Search Guard roles

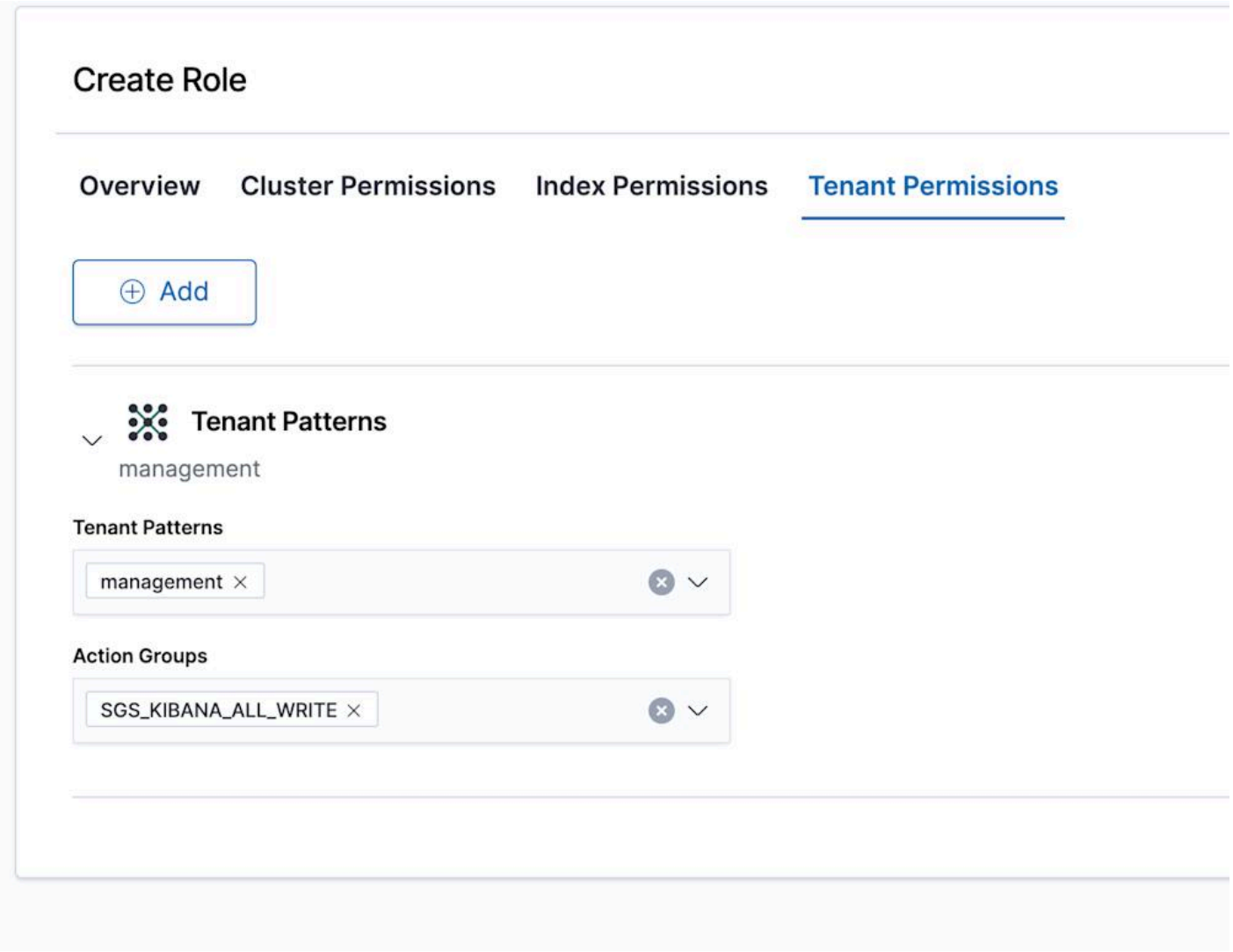
Next, we want to define which users should have access to the tenant. As with all other permission settings, access to tenants is configure per Search Guard role.

To grant a Search Guard role access to one or more tenants, create a new role or edit an existing one. A role has three sections regarding access permissions:

- **Cluster permissions**: Controls cluster-wide operations like stats or health
- **Index permissions**: Controls access to indices
- **Tenant permissions**: Controls access to Kibana tenants

To grant access to the newly created "management" tenant, we choose "Tenant Permission" from the menu.

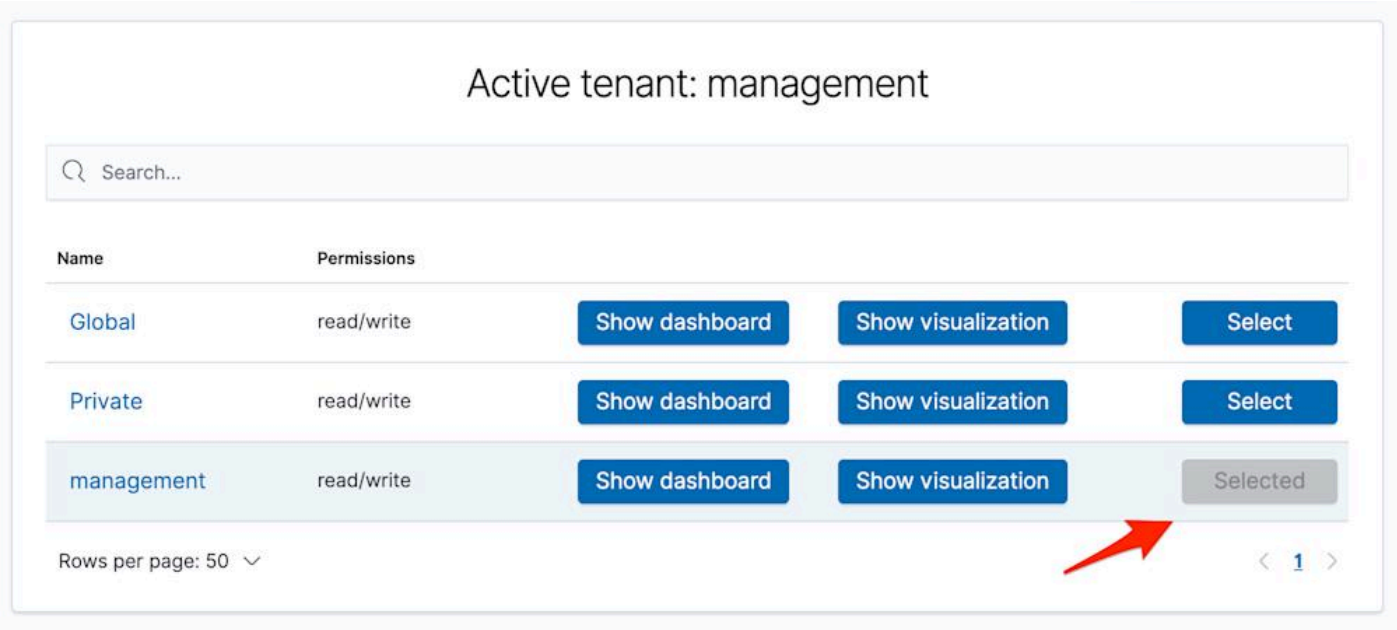
In the following screen, we add the "management" tenant to our role. As "action group," we choose SGS_KIBANA_ALL_WRITE. Any user with this role now has read/write permissions for Saved Objects in the "management" tenant.



Instead of choosing SGS_KIBANA_ALL_WRITE you can also use SGS_KIBANA_ALL_READ. This would grant the role read-only access to Saved Objects in the tenant.

Selecting tenants

We now log in to Kibana with a user that has the Search Guard role from above assigned. We choose "Tenants" from the left-hand Kibana navigation. In the next screen, we see all tenants the user has access to, including our newly create "management" tenant. To activate the tenant, we click on "Select".



Every object the user creates, like Dashboards or Visualizations, is now saved in the "management" tenant. Only users that have access to this tenant can view and modify these objects.

Where to go next

- Read the Kibana Multi-Tenancy documentation
- If you run into any problem, refer to our Multi Tenancy Troubleshooting guide
- Ask any questions related to Multi Tenancy on our Search Guard forum

Image: shutterstock / Irzhanova Asel

This article was published on the Search Guard blog: https://search-guard.com/blog/kibana-tenants/
Search Guard is Security and Alerting for Elasticsearch and Kibana — search-guard.com · Start a free trial