Kibana Multi Tenancy with Search Guard

Jochen Kressin · 2018-10-08

Kevin and Jessie work at the same company. Kevin has been asked to prepare Kibana dashboards for Jessie. Kevin needs to be able to create and alter dashboards and visualizations while Jessie should be only able to view them. This seems to be an everyday use case, however, at the time of writing Kibana does not implement it out of the box. Fortunately, this is possible thanks to Kibana Multitenancy feature implemented within Search Guard.

Tenant Concept

Kibana stores its objects in a single index which is by default called *.kibana*. Each Kibana user can access all of the objects. Search Guard introduces the *tenant* concept. Each tenant is a named container for saved objects. Technically, each tenant becomes a separate index and Search Guard guarantees it's security as separation is done directly in Elasticsearch.

Enabling multitenancy

We start our demo with a fresh installation of ElasticSearch and Kibana, both with Search Guards plugins installed. We load the accounts dataset from the Elasticsearch tutorial, which contains 1000 sample bank accounts records. Once *acccounts.zip* file is downloaded locally and unpacked, this can be done with the command:

```
curl -H 'Content-Type: application/x-ndjson' -k -u admin:admin -XPOST 'https://<es-
host>:9200/bank/account/_bulk?pretty' --data-binary @accounts.json
```

We follow the Search Guard instruction steps to allow Kibana multitenancy. We modify *kibana.yml* by setting:

```
multitenancy_enabled: true
elasticsearch.requestHeadersWhitelist: [ "Authorization", "sgtenant" ]
```

and *sg_config.yml* with

```
searchguard.multitenancy.enabled: true
```

Demo users and roles

We create two roles in *sg_roles.yml*:

```
sg_account_resources_rw:
  indices:
    '*':
      '*':
        - indices:data/read/get
        - indices:data/read/search
    'bank':
      '*':
        - READ
  tenants:
    sg_account_resources: RW
```

and

```
sg_account_resources_ro:
  indices:
    '*':
      '*':
        - indices:data/read/get
        - indices:data/read/search
    'bank':
      '*':
        - READ
  tenants:
    sg_account_resources: RO
```

This allows both groups to access the *bank* index and defines a tenant *sg_account_resources* - a location of Kibana objects. Both groups share the location with different permissions: read-write (RW) and read-only (RO).

We map these roles in *sg_roles_mapping.yml*:

```
sg_account_resources_rw:
  backendroles:
    - sg_account_resources_rw

sg_account_resources_ro:
  backendroles:
    - sg_account_resources_ro
```

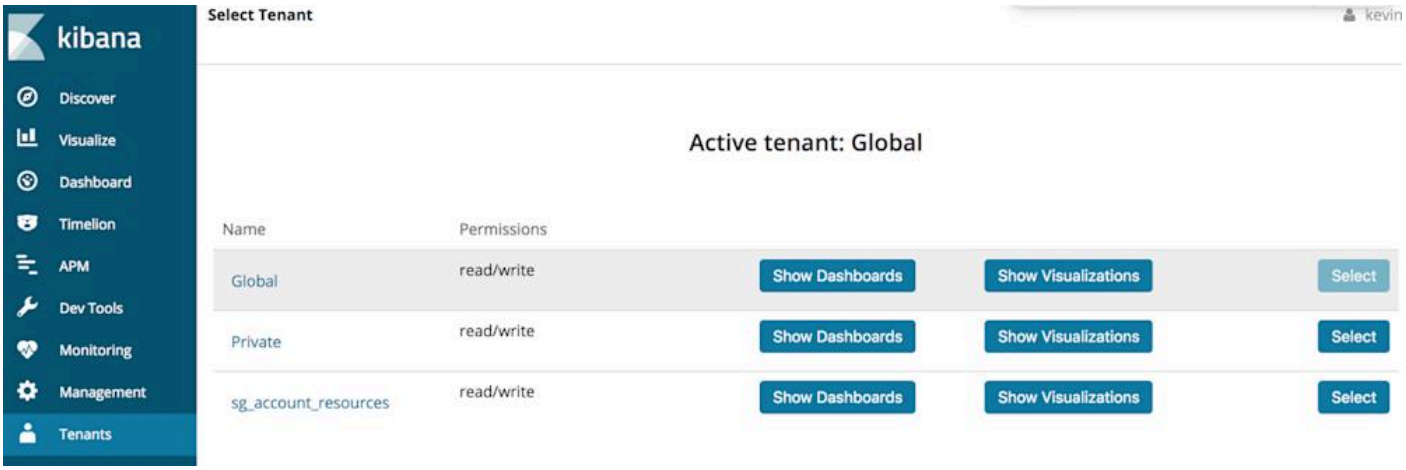
Then we can add Kevin and Jessie users in *sg_internal_users.yml*:

```
kevin:
  hash: $2y$12$JwORr3rXHi4GuB8K6NXOpe1PwdU1m7MiNIERem02/bgcIJMaKDj1K
  roles:
    - kibanauser
    - sg_account_resources_rw

jessie:
  hash: $2y$12$JwORr3rXHi4GuB8K6NXOpe1PwdU1m7MiNIERem02/bgcIJMaKDj1K
  roles:
    - kibanauser
    - sg_account_resources_ro
```

Selecting Tenants

When Kevin logs into Kibana, *Tenants* section is available in menu:

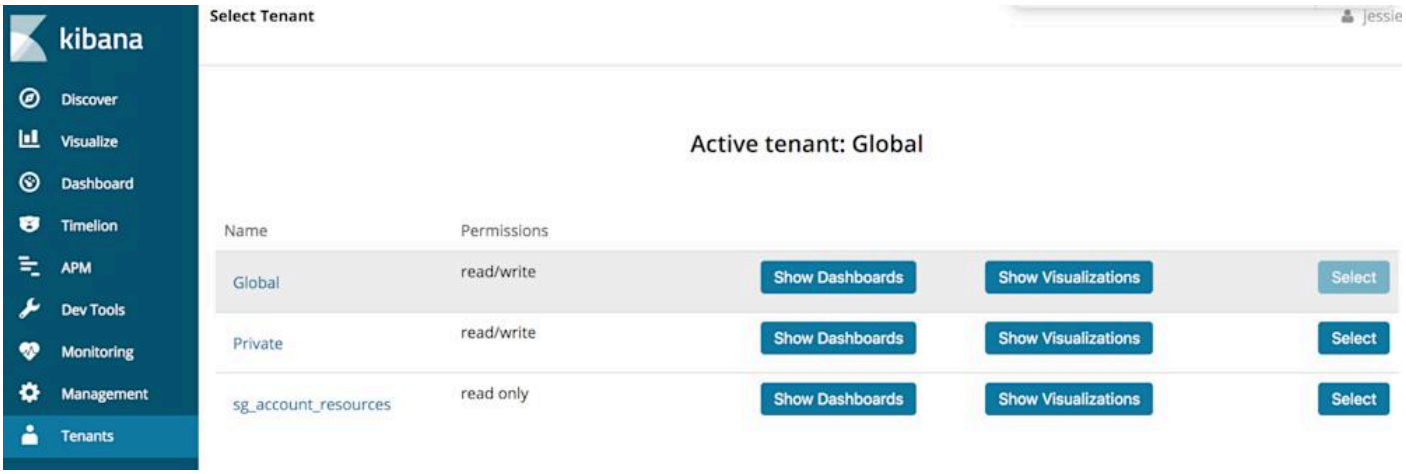


There are three tenants available:

- *Global* - Kibana objects shared among all users
- *Private* - accessible only by Kevin
- *sg*\account_resources_ - defined by us with read/write permissions.

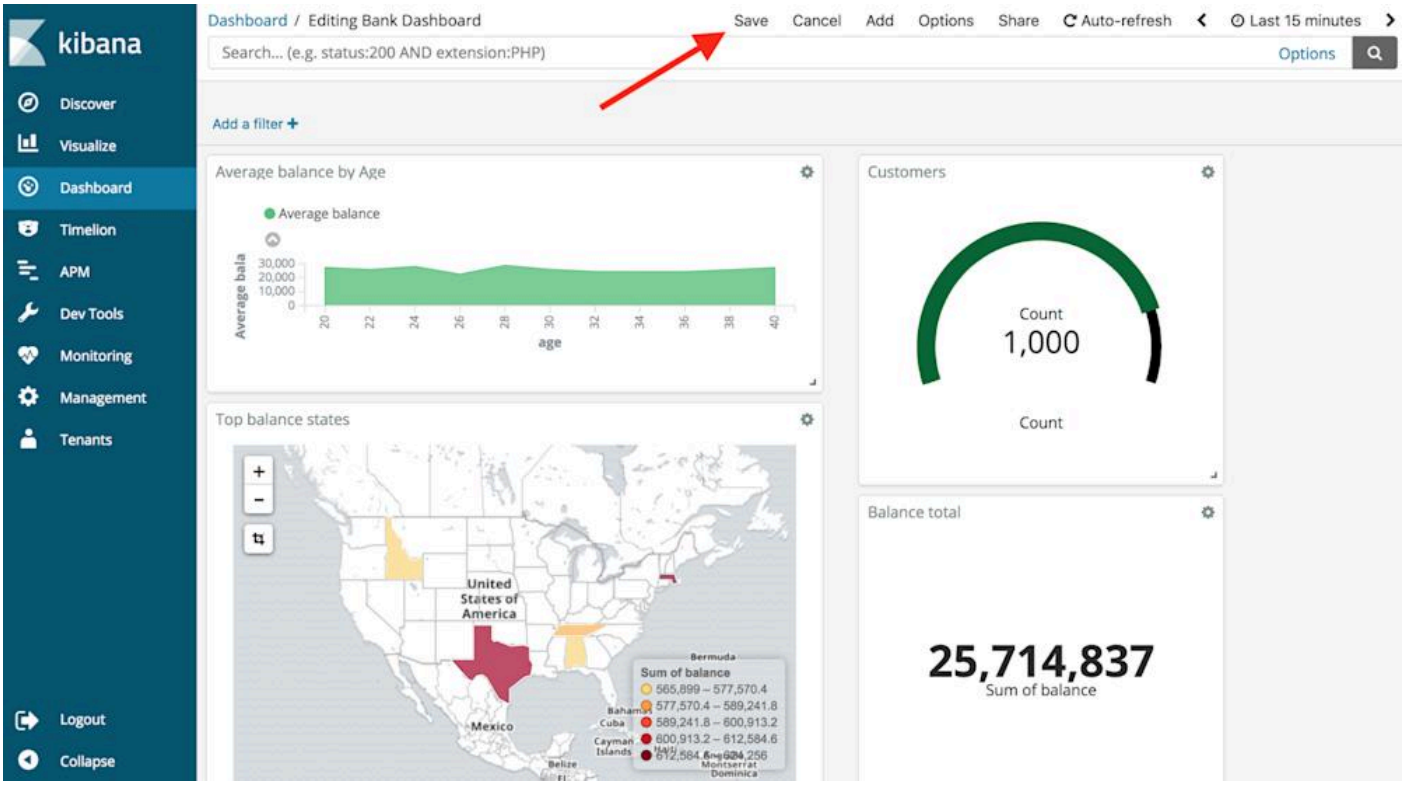
Kevin needs to select a *sg_account_resources* tenant. Additionally, Search Guard allows to specify a default tenant or give an URL to Kibana which automatically selects the given tenant.

Jessie's *tenants* section looks similar but *sg_account_resources* tenant permissions are restricted to read only:

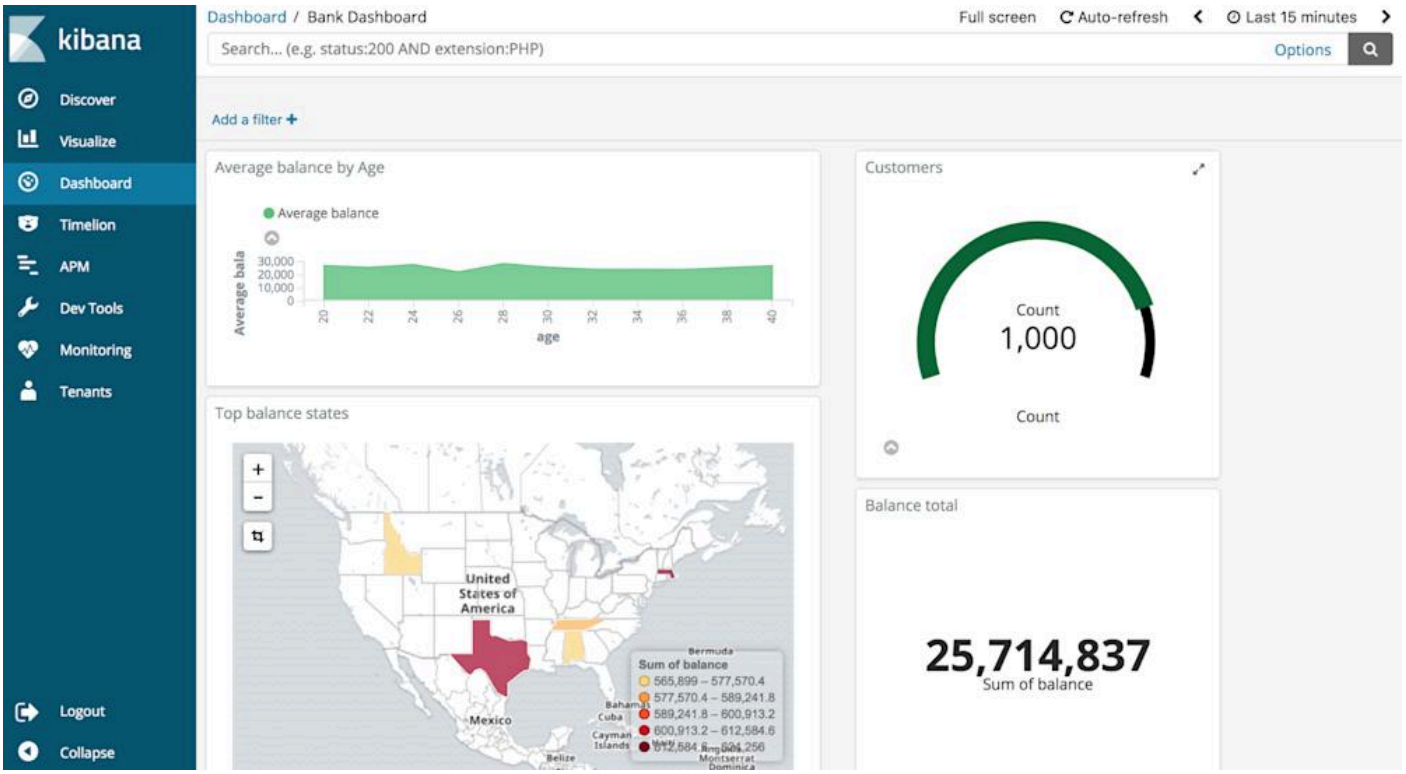


Tenant permissions

Kevin needs to create a separate index-mapping within a tenant so that he can create a dashboard like the one below. One can see the Save button on the top menu that is available for Kevin.



When Jessie logs in and views the same dashboard, it cannot be modified by her.



Where to go next:

- Read about all multitenancy configuration options in the official documentation
- If you have problems setting up multitenancy, follow our troubleshooting guide
- If you have questions, head over to the Search Guard forum

Image: shutterstock / pizzastereo

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