

# LAB 3 – Elasticsearch Security

*Estimated Time for This Lab: 45 Min*

## Introduction

Log data may contain sensitive information that needs to be secured.

To prevent unauthorized access to your Elasticsearch cluster, you must have a way to authenticate users. This simply means that you need a way to validate that a user is who they claim to be. For example, you have to make sure only the person named Kelsey Andorra can sign in as the user kandorra. Elastic security provides a standalone authentication mechanism that enables you to quickly password-protect your cluster. If you're already using LDAP, Active Directory, or PKI to manage users in your organization, Elastic security is able to integrate with those systems to perform user authentication.

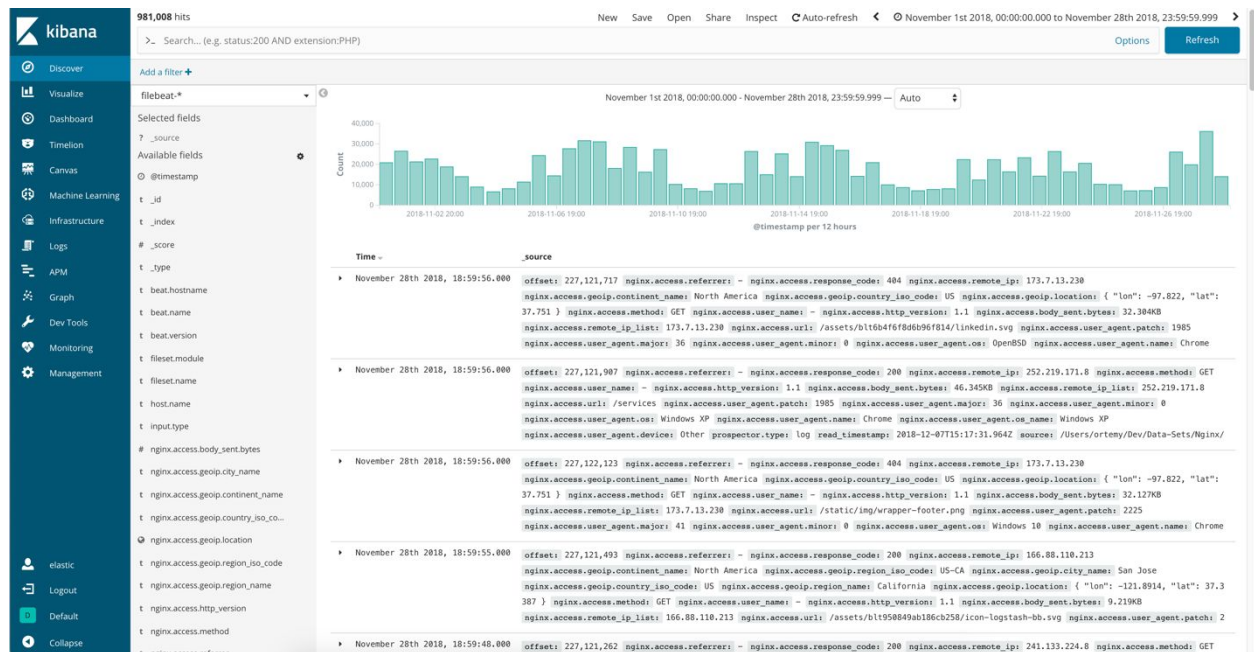
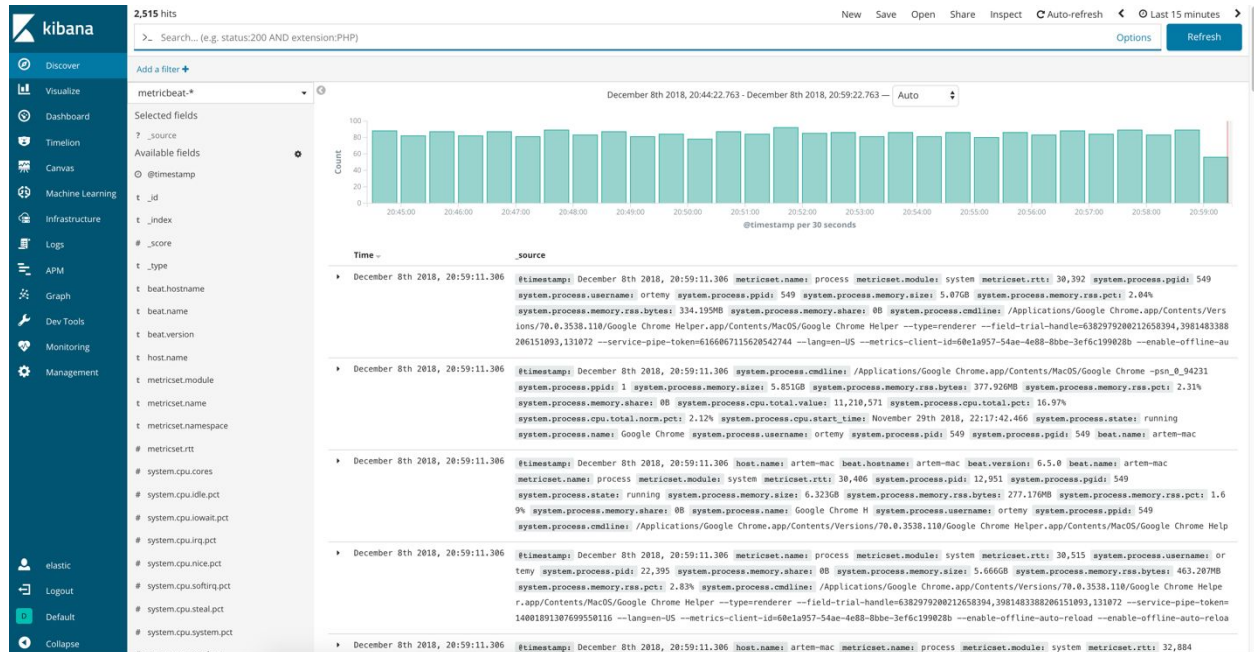
We have been using Elastic security to log into your Elasticsearch Service clusters during lab 1 and 2.

In many cases, simply authenticating users isn't enough. You also need a way to control what data users have access to and what tasks they can perform. Elastic security enables you to authorize users by assigning access privileges to roles, and assigning those roles to users. For example, this role-based access control mechanism (a.k.a RBAC) enables you to specify that the user kandorra can only perform read operations on the events index and can't do anything at all with other indices.

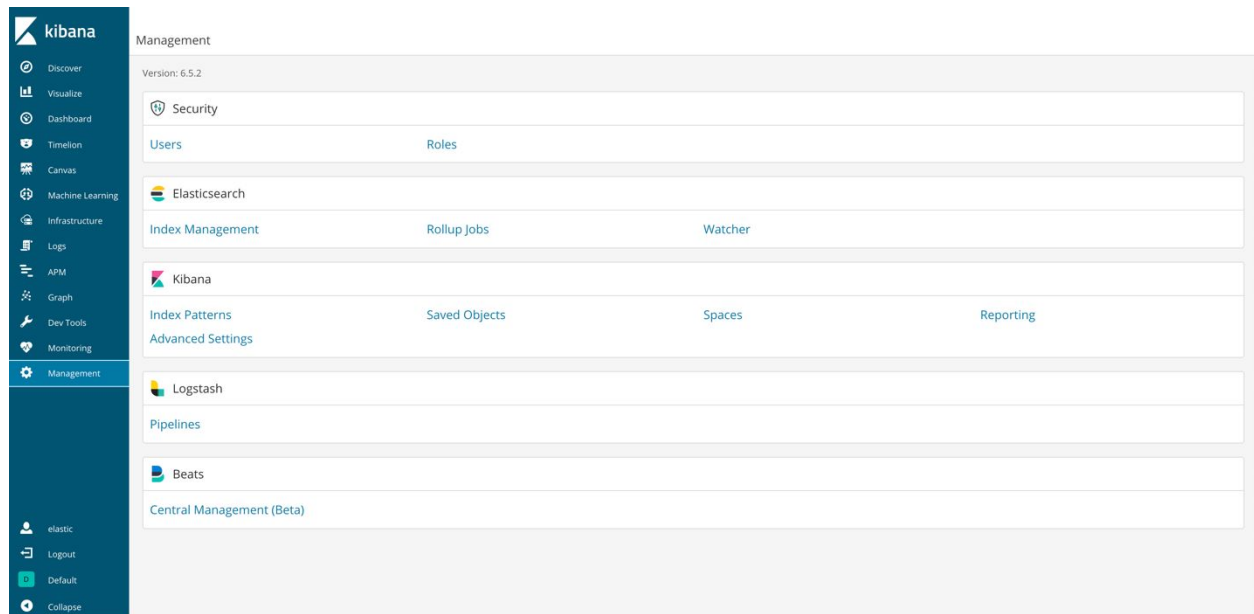
In this Lab we will use Elastic Security to restrict access to your log data.

Let's get started!

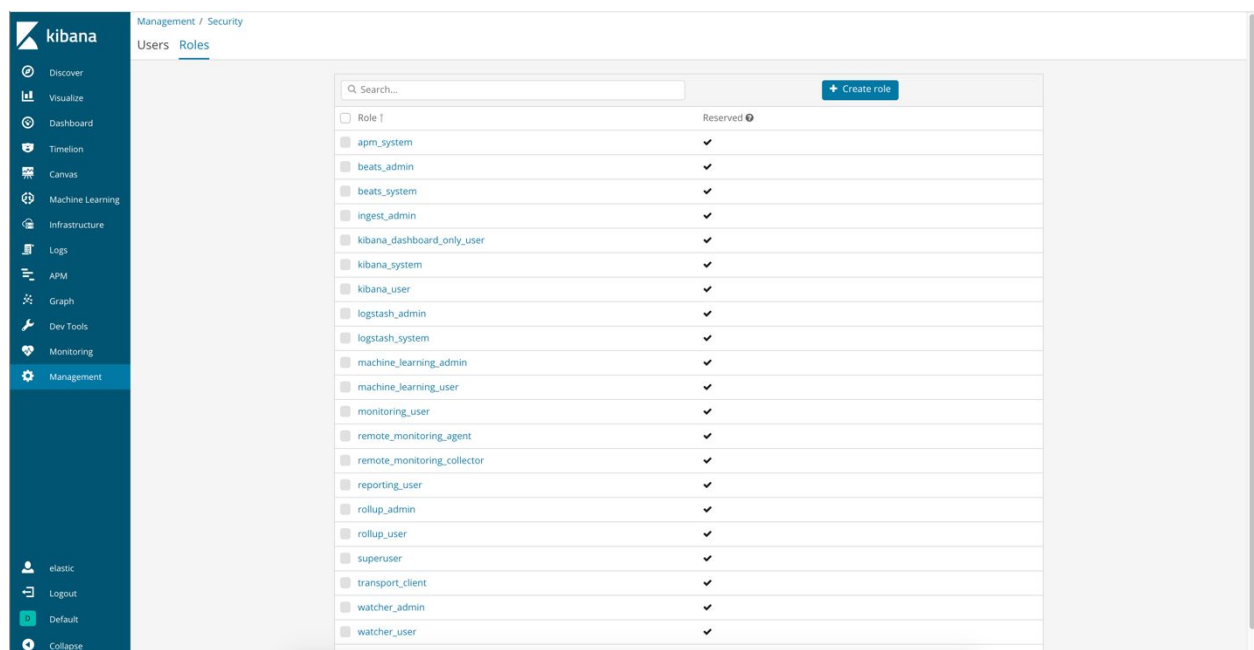
1. In Kibana click on “Discover” item in the menu. Select “filebeat-\*” and “metricbeat-\*” index pattern. When selecting “filebeat-\*” use date range “Nov 1<sup>st</sup>, 2018 – Nov 28<sup>th</sup>, 2018”. When selecting “metricbeat-\*” use “Last 15 min”.



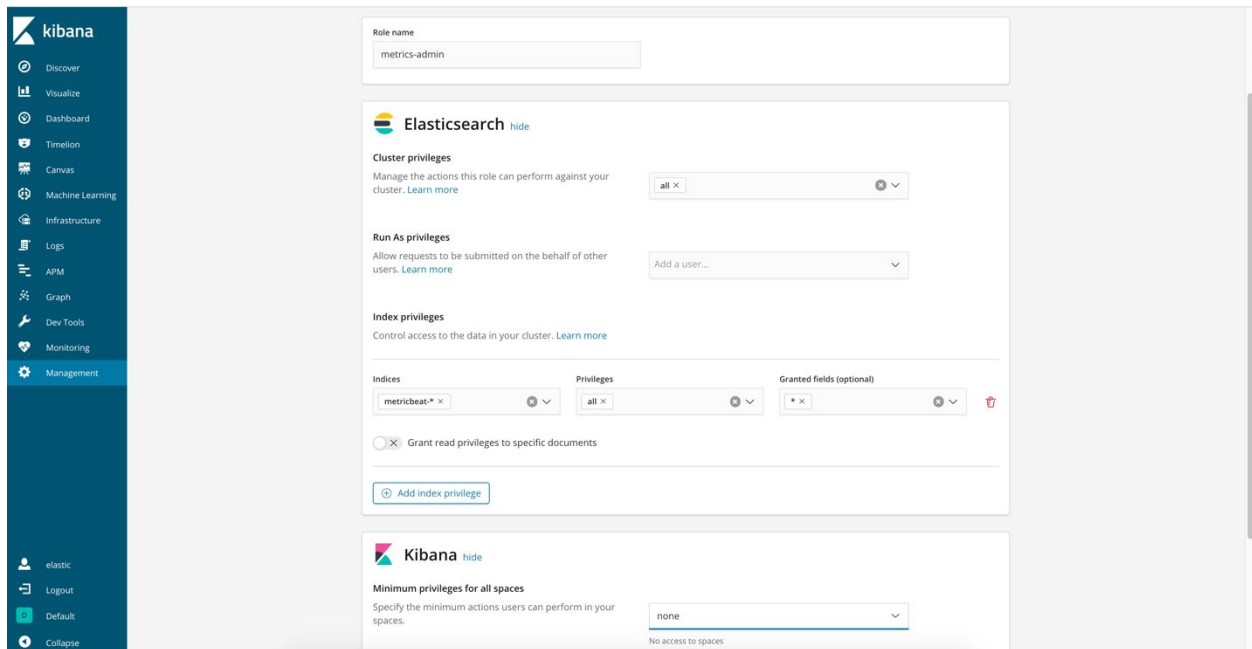
2. What if these use cases belong to different groups (metrics and logs for example) and compliance requires to hide logs from metrics group? How do we achieve that? The way to do that with the Elastic Security tool. Click on “Management” item on the Kibana menu.



3. Under Security click on Roles and then click on “Create Role”.

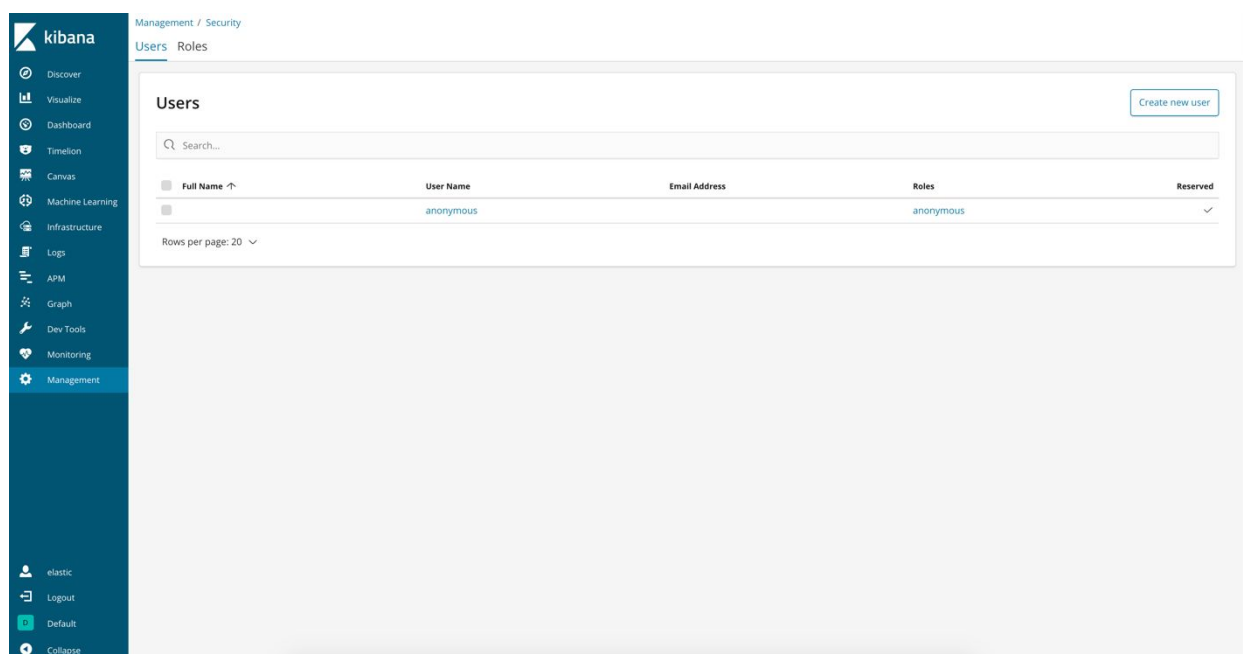


4. Give your new role a name (“metrics-admin” for example). Under cluster privileges select “all”, under Indices select “metricbeat-\*”, under index privileges select “all”. Click on “Create role”.

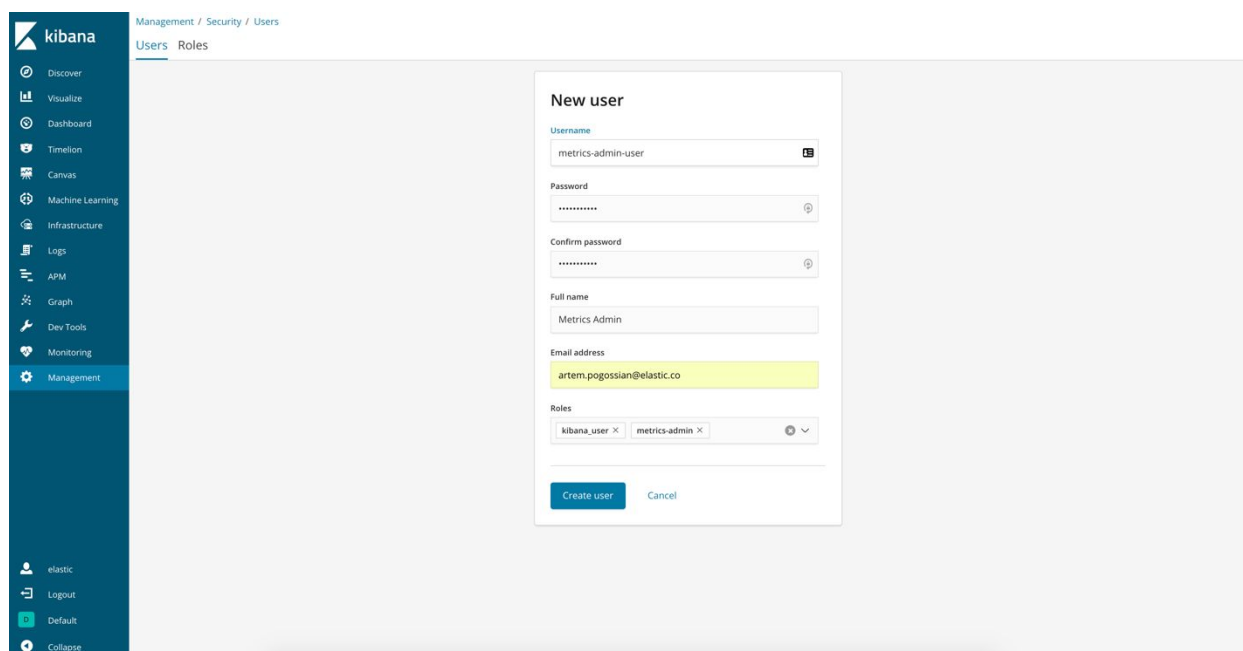


The screenshot shows the Kibana Security console interface. On the left is a sidebar with the Kibana logo and a menu including Discover, Visualize, Dashboard, Timeline, Canvas, Machine Learning, Infrastructure, Logs, APM, Graph, Dev Tools, Monitoring, and Management (which is highlighted). Below the menu are links for elastic, Logout, Default, and Collapse. The main content area is titled 'Role name' with a text input field containing 'metrics-admin'. Below this is the 'Elasticsearch' section with three privilege categories: 'Cluster privileges' (set to 'all'), 'Run As privileges' (set to 'Add a user...'), and 'Index privileges'. The 'Index privileges' section has three sub-sections: 'Indices' (set to 'metricbeat-\*'), 'Privileges' (set to 'all'), and 'Granted fields (optional)' (set to '\*'). There is a checkbox for 'Grant read privileges to specific documents' which is unchecked. Below these is a button 'Add index privilege'. The bottom section is titled 'Kibana' and 'Minimum privileges for all spaces', with a dropdown menu set to 'none' and a note 'No access to spaces'.

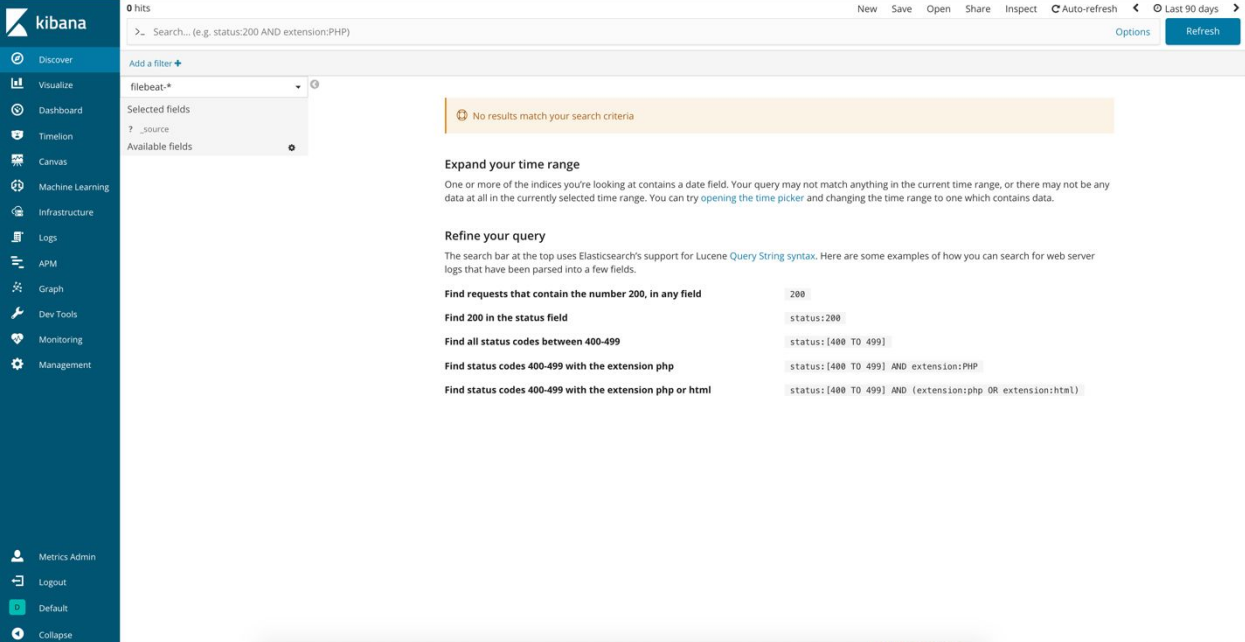
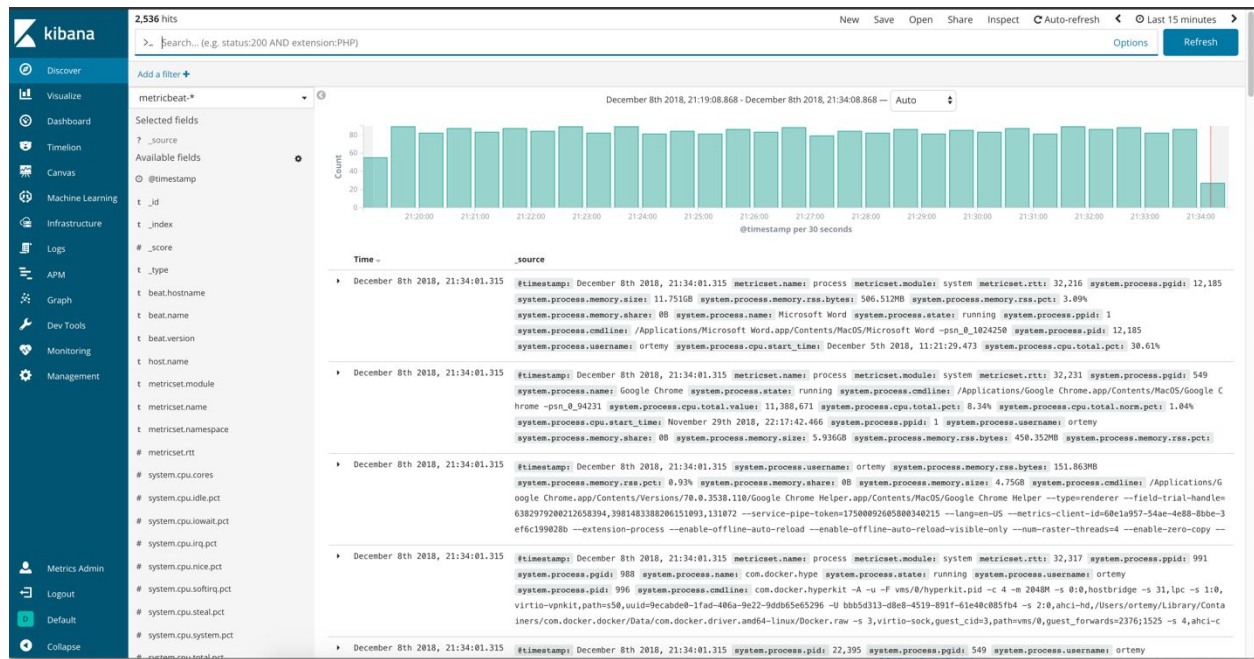
5. After the role is created click on “Management” tab on Kibana menu again, but under Security section this time click on “Users”. Click on “Create new user”.



6. Give it a username and a password, full name, and email. In the roles assigned to the user select “kibana-user” and “metrics-admin”. Click on “Create User” button.



7. From another browser (or same browser incognito mode) login to that same cluster with the newly created user credentials. Once you login click on “Discover” tab on Kibana menu. Note that the only index pattern you can see data for is “metricbeat-\*” and for “filebeat-\*” index pattern you cannot see any data.



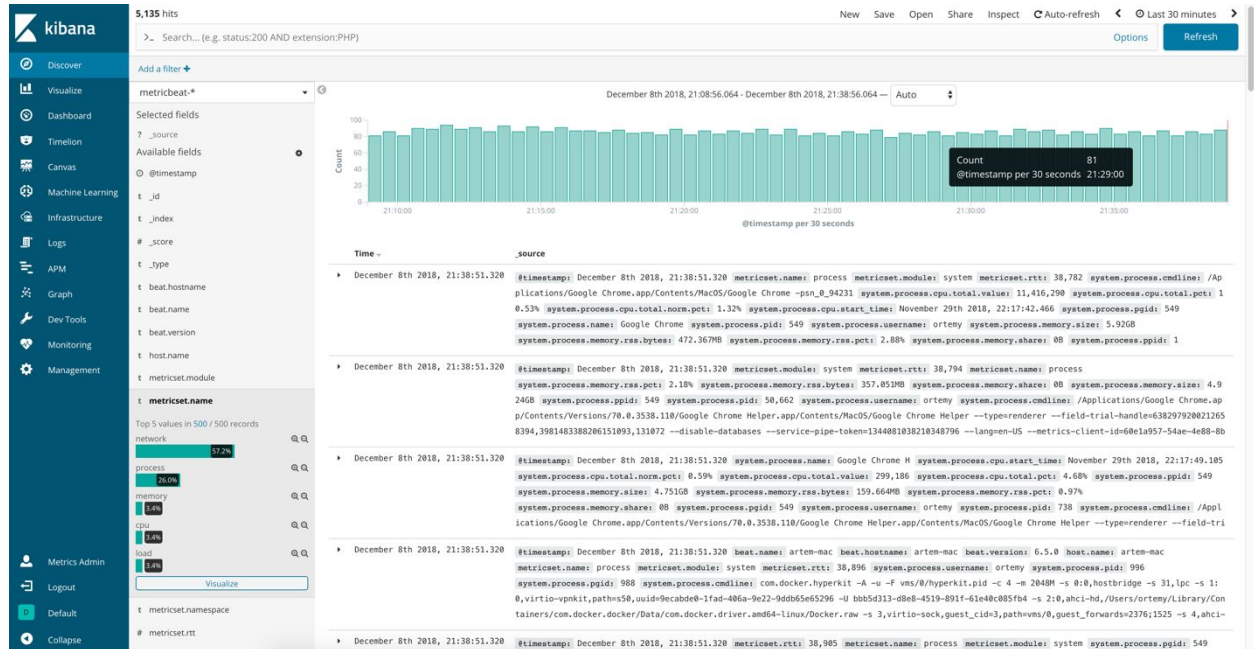
The Kibana dashboard displays search results for the query `filebeat-*`. The top section shows a message: `No results match your search criteria`. Below this message, there is a section titled `Expand your time range` with a description: `One or more of the indices you're looking at contains a date field. Your query may not match anything in the current time range, or there may not be any data at all in the currently selected time range. You can try opening the time picker and changing the time range to one which contains data.` Below this section, there is a section titled `Refine your query` with a description: `The search bar at the top uses Elasticsearch's support for Lucene Query String syntax. Here are some examples of how you can search for web server logs that have been parsed into a few fields.` Below this section, there are several examples of search queries and their corresponding results:

- `Find requests that contain the number 200, in any field` results in `200`
- `Find 200 in the status field` results in `status:200`
- `Find all status codes between 400-499` results in `status:[400 TO 499]`
- `Find status codes 400-499 with the extension php` results in `status:[400 TO 499] AND extension:PHP`
- `Find status codes 400-499 with the extension php or html` results in `status:[400 TO 499] AND (extension:php OR extension:html)`

Note, that index pattern “filebeat-\*” is still visible. The way to assign permissions to objects is by using new feature in Kibana 6.5 called “Kibana Spaces”. We will demo this feature in the end of this lab.



8. Select “metricbeat-\*” index pattern again. Click on the field “metricset.name” to see all the available metrics for the system that we are collecting.

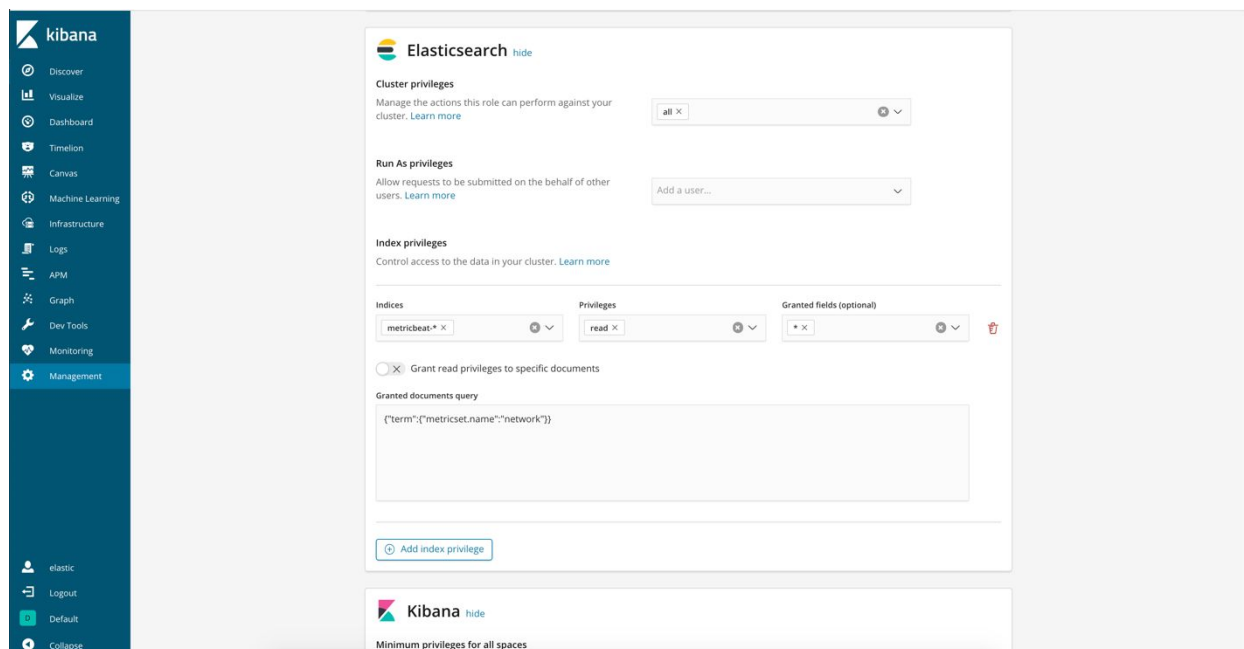


9. One of the data types we are collecting is “network”. Imagine a scenario in which we have network operations users that are only allowed to see networking data and nothing else. Can we provide them document level access based on this attribute (document level security)? Login as “elastic” user again (or switch to another browser window where you still have that session active) and create a new role with the name “network-user”.

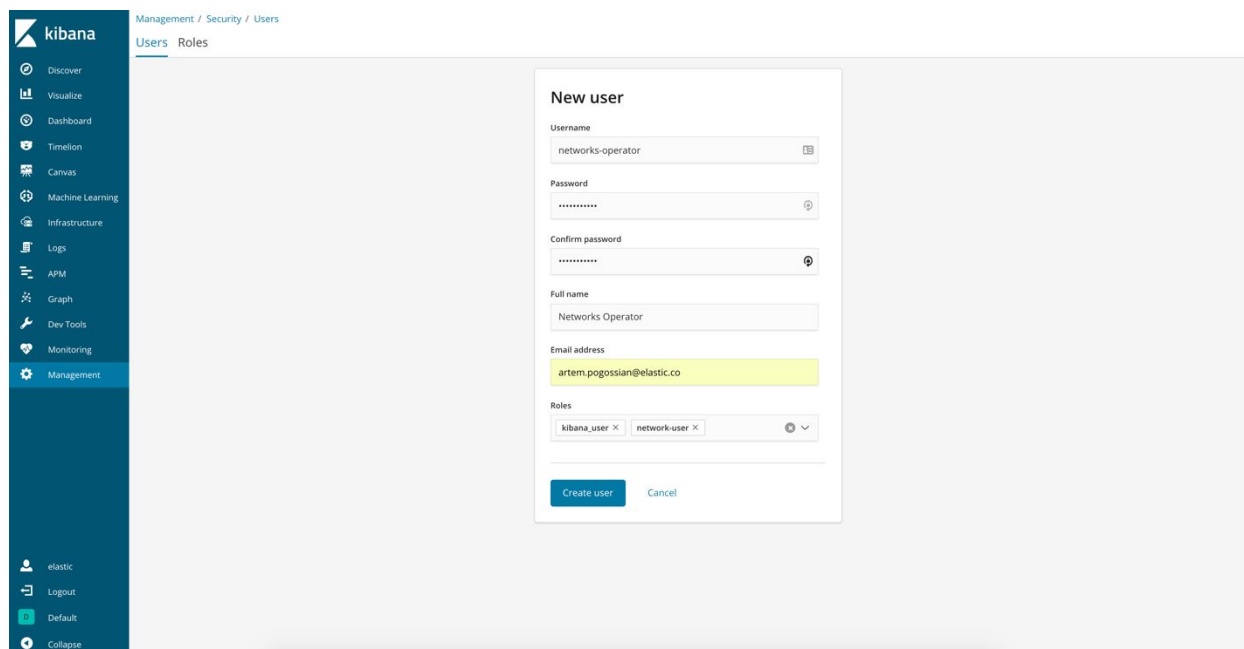
Set the following values:

- Cluster privileges : all
- Indices: metricbeat-\*
- Index Privileges: read
- Click on: **Grant read privileges to specific documents**
- In the query box type in the following query: `{ "term": { "metricset.name": "network" } }`

Click on “Create Role”.



10. Create a user with this new role, don't forget to assign "kibana-user" to it too, otherwise this newly created user will only be allowed access to Elasticsearch APIs.

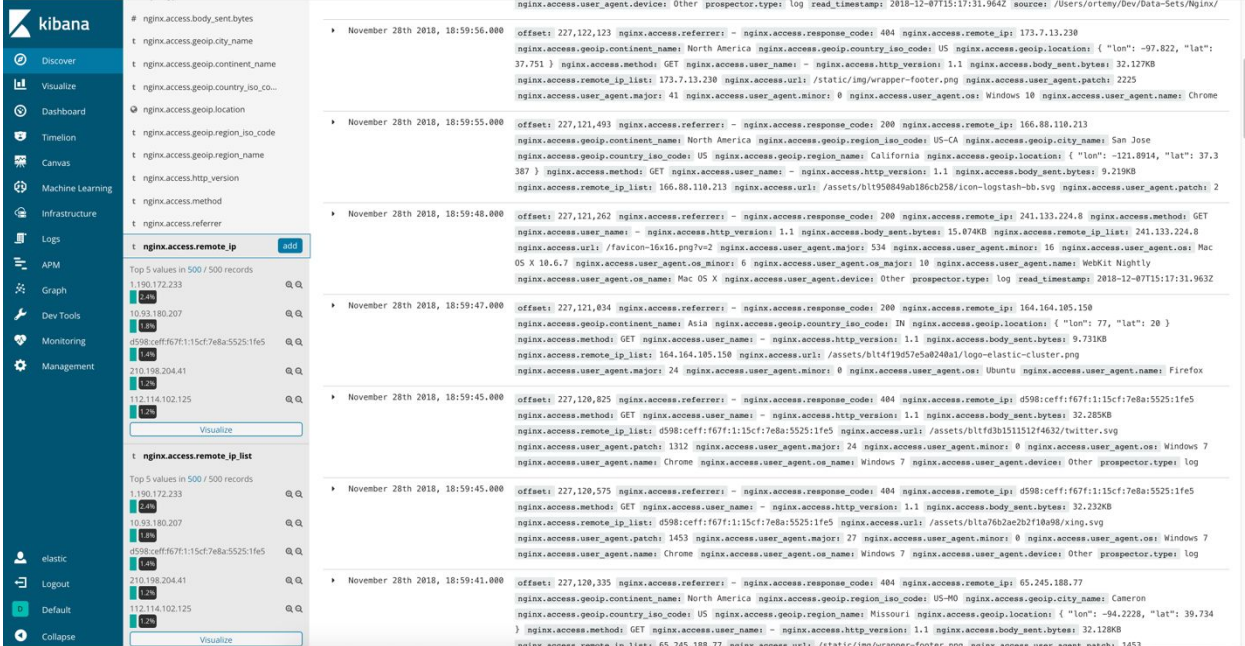


11. Login as this newly created user, click on Discover and select "metricbeat-\*" index pattern. Expand "metricset.name" field by clicking on it and note how the only value



[illegible]

- Page: Lab 3 - 9

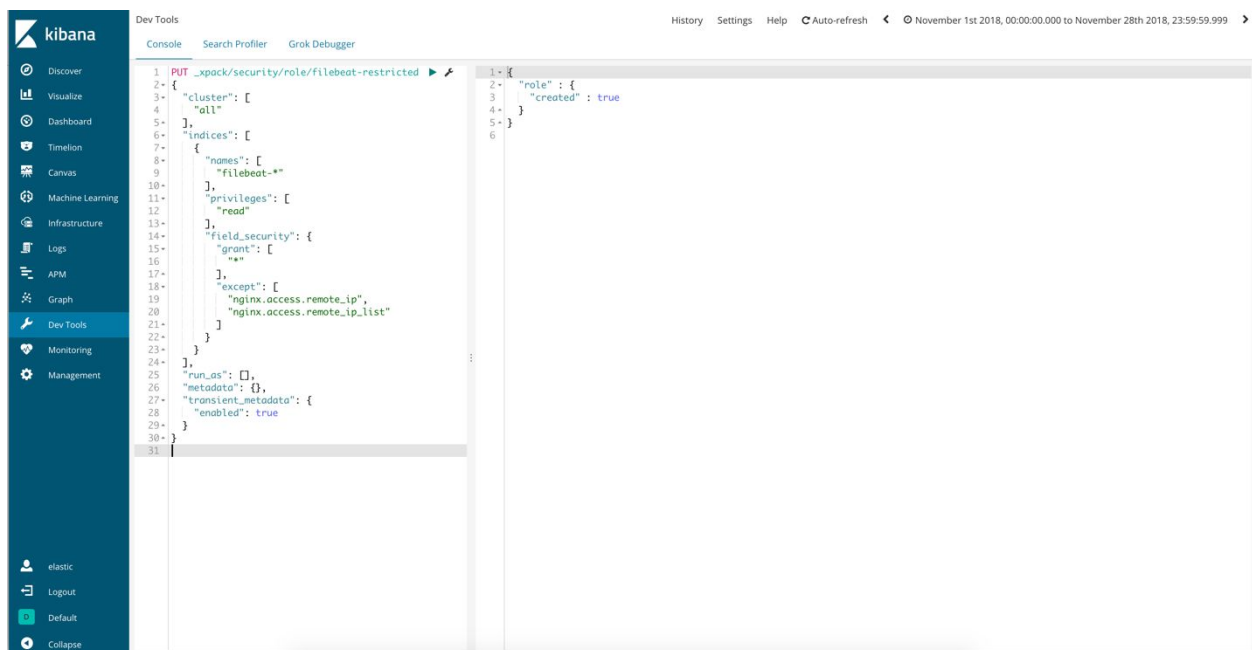


How can we achieve that? Let's create a new role where we would hide this field. But this time let's actually explore API Capabilities of Elasticsearch. Click on "Dev Tools" item on the Kibana menu and paste this code snippet:

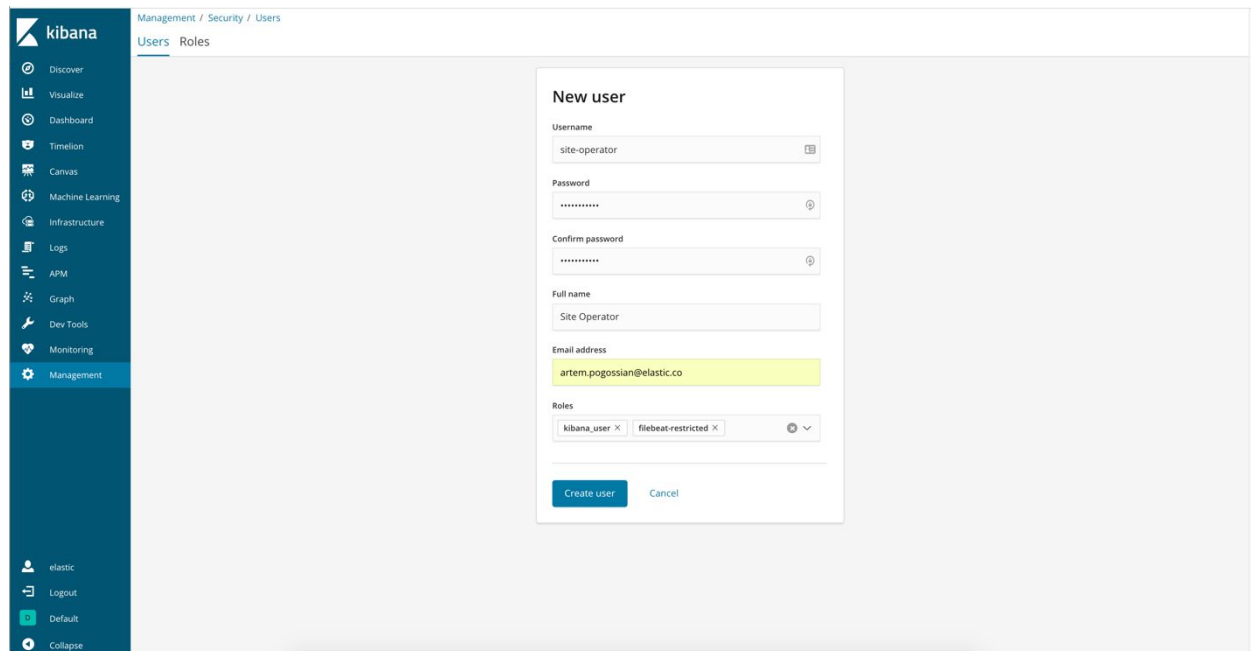
```
PUT _xpack/security/role/filebeat-restricted
{
  "cluster": [
    "all"
  ],
  "indices": [
    {
      "names": [
        "filebeat-*"
      ],
      "privileges": [
        "read"
      ],
      "field_security": {
        "grant": [
          "*"
        ],
      },
    }
  ],
}
```

```
    "except": [
      "nginx.access.remote_ip",
      "nginx.access.remote_ip_list"
    ]
  }
},
"run_as": [],
"metadata": {},
"transient_metadata": {
  "enabled": true
}
}
```

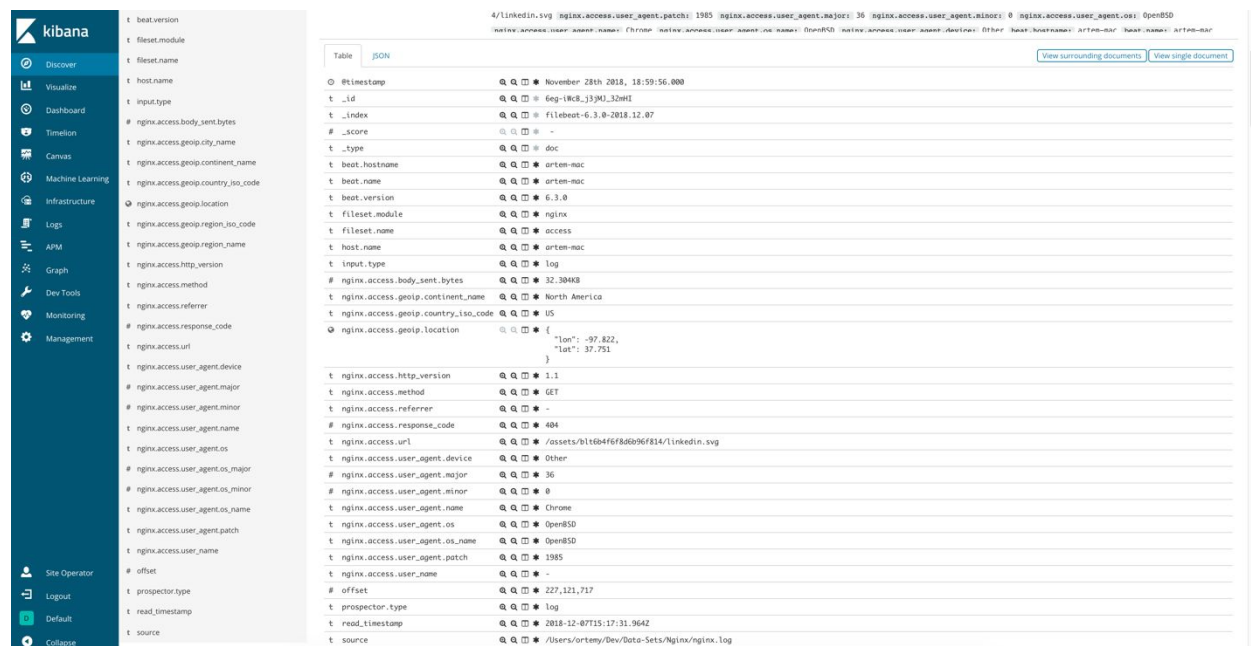
Execute the API call.



Once the role is created, create a user “site-operator” and assign this role to the user.



Login as this newly created user, click on “Discover” and select “filebeat-\*” index pattern. Note how none of IP fields no longer appear on the left-hand side menu and inside the actual documents.



## Summary

In this Lab we will use Elastic Security to restrict access to your log data at the index; field and document level.