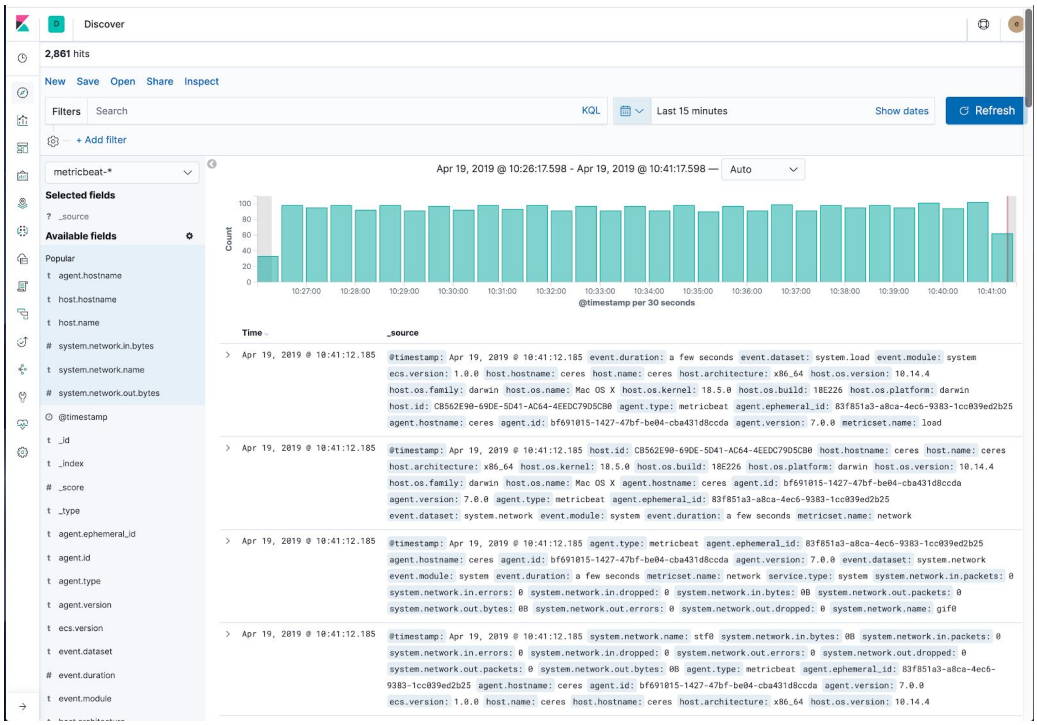
Elastic Observability Workshop

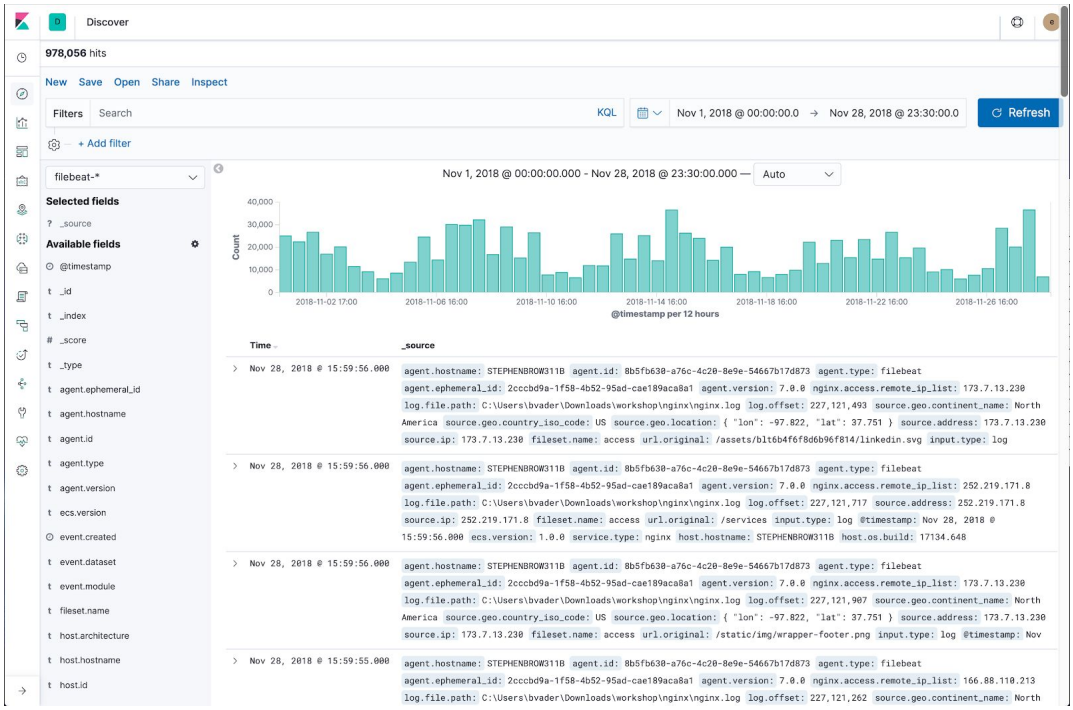
Lab 3 - Security

1) In Kibana click on “Discover” item in the menu. Toggle between **`filebeat-*`** and **`metricbeat-*`** index pattern. When selecting **`filebeat-*`**use date range **`Nov 1st, 2018 – Nov 28th, 2018`**. When selecting **`metricbeat-*`** use **`Last 15 min`**.

Metricbeat

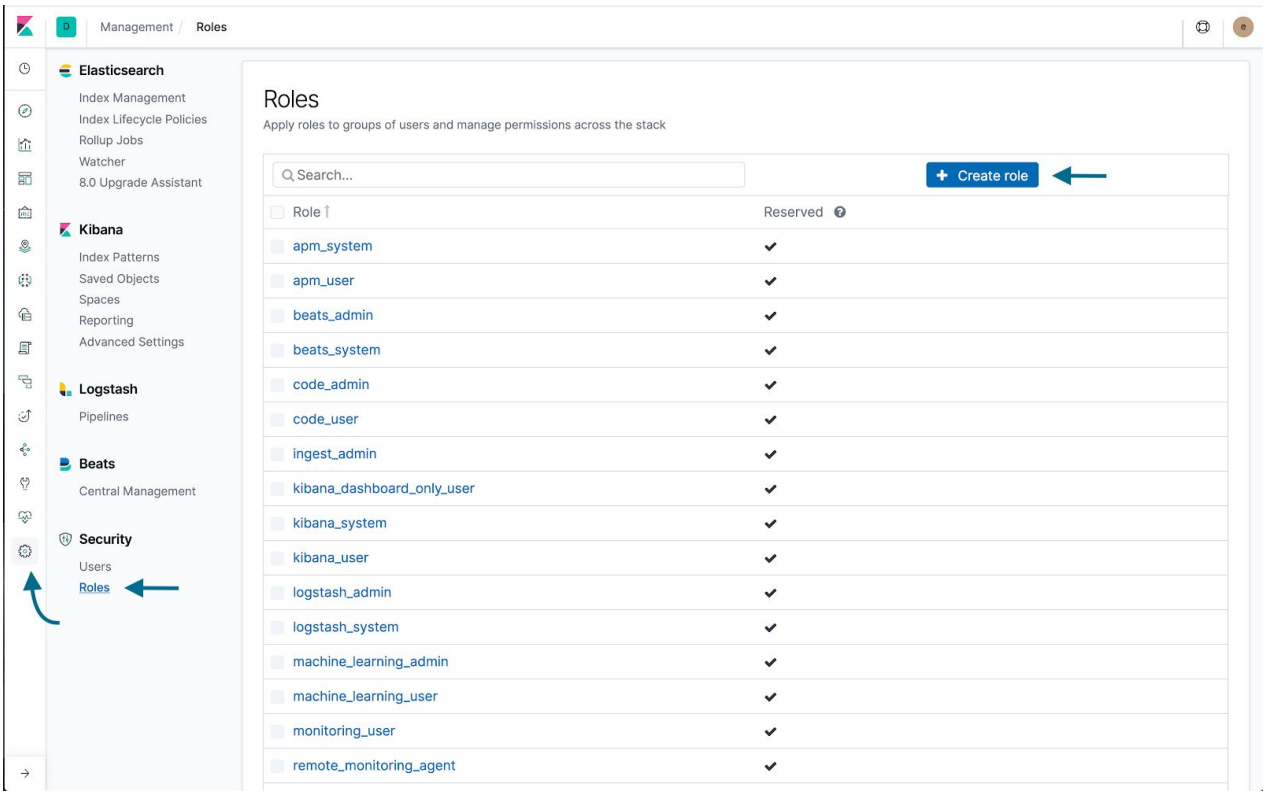


Filebeat

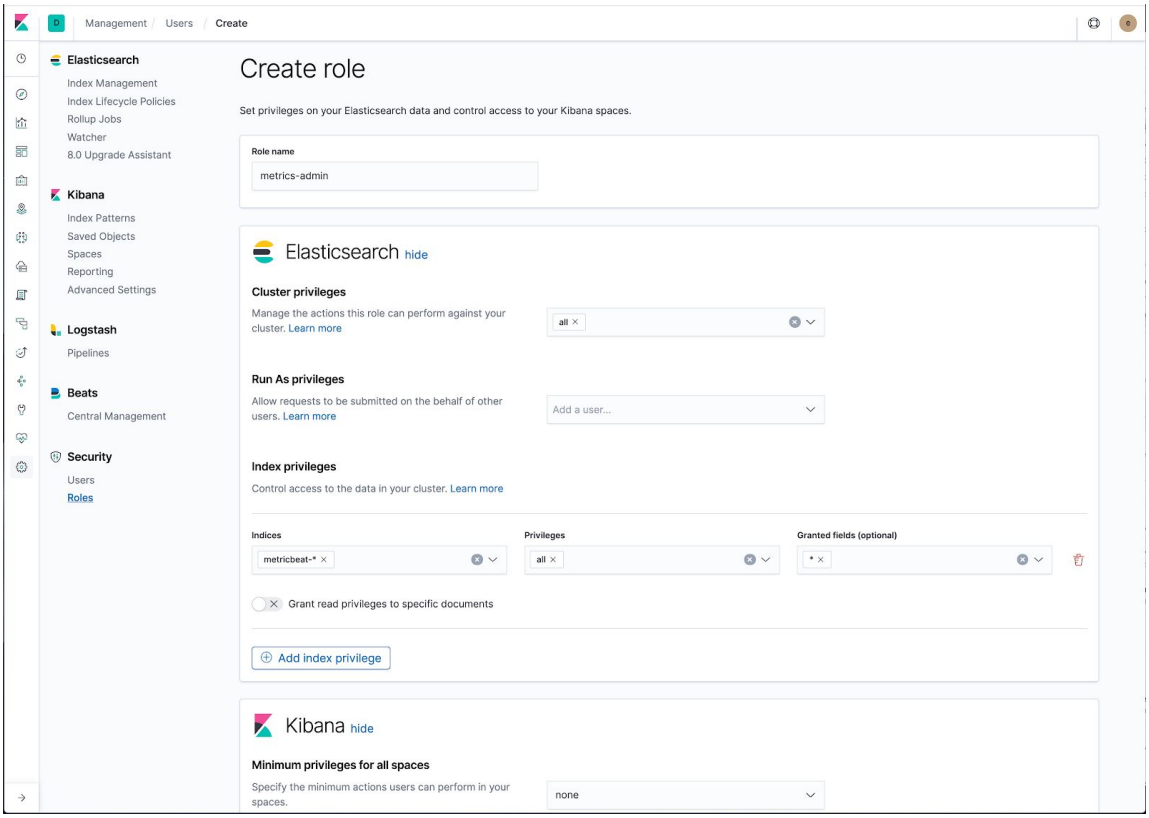


2) What if these use cases belong to different groups (metrics and logs for example) and compliance requires to hide logs from metrics group? How do we achieve that? We can use Elastic's security capabilities to achieve that. Click on "Management" item on the Kibana menu.

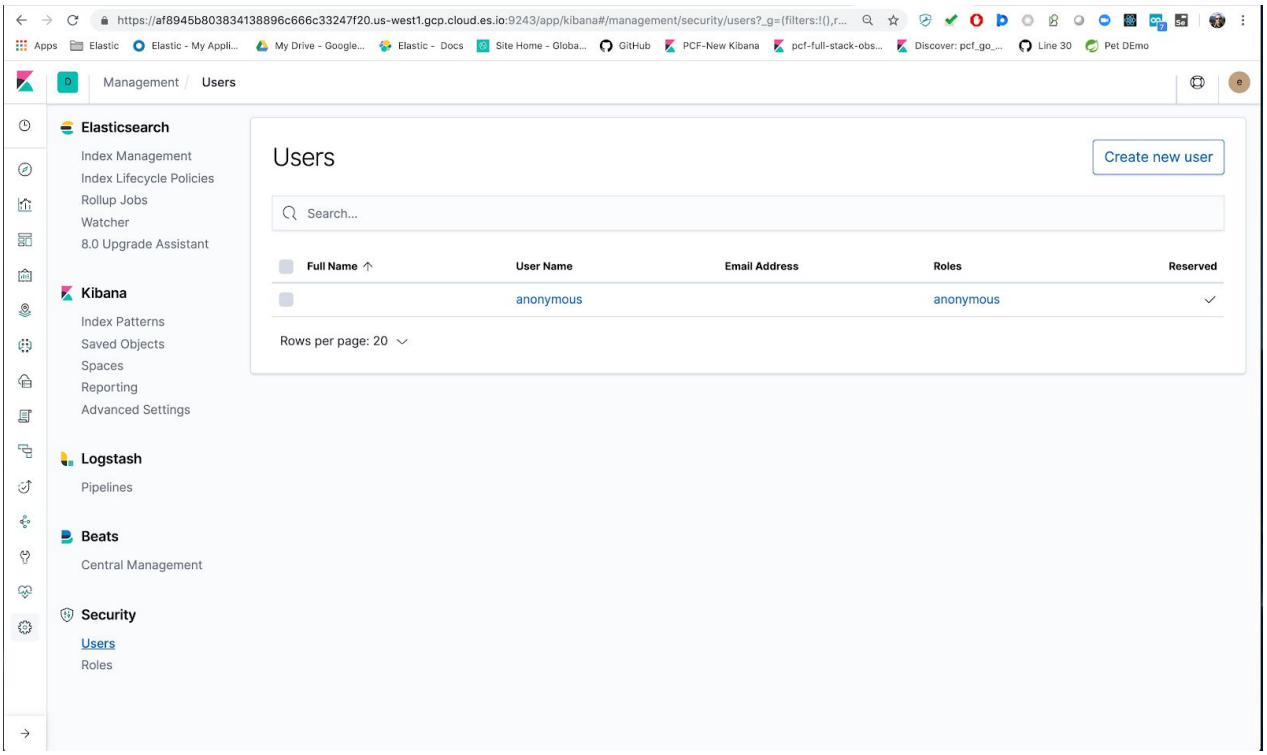
3) Under Security click on Roles and then click on "Create Role".



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`**. Scroll to the bottom and click on **`Create role`**

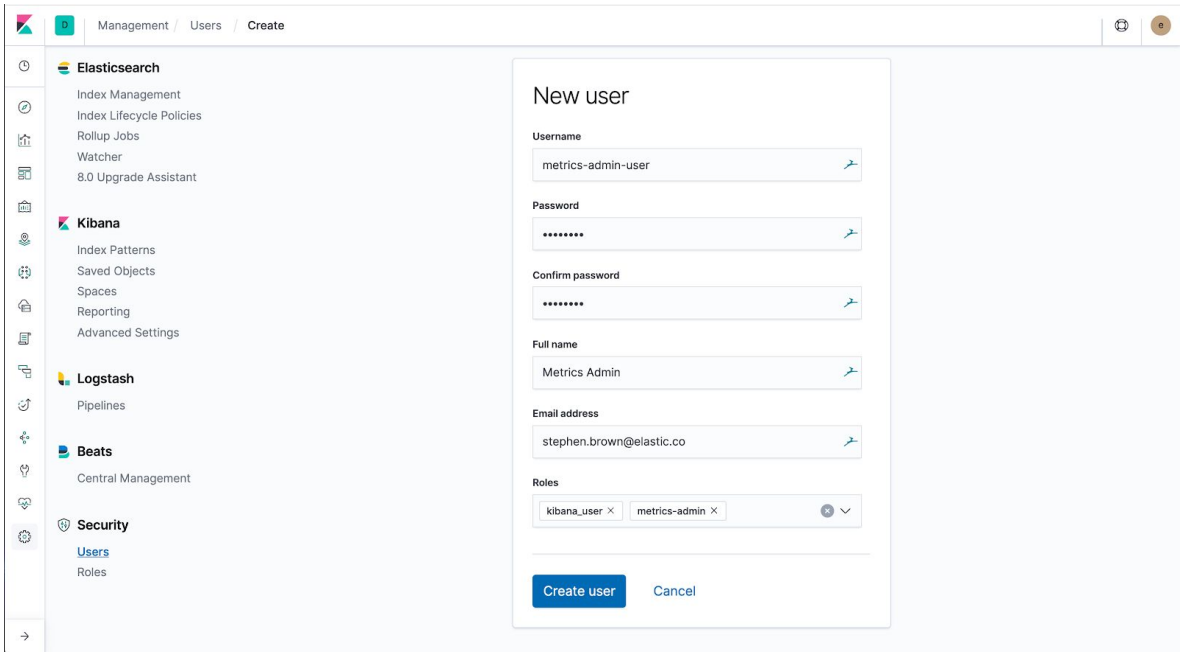


5) After the role is created click on **`Management`** tab on Kibana menu again. Under **`Security`** section this time click on **`Users`**. Click on **`Create new user`**



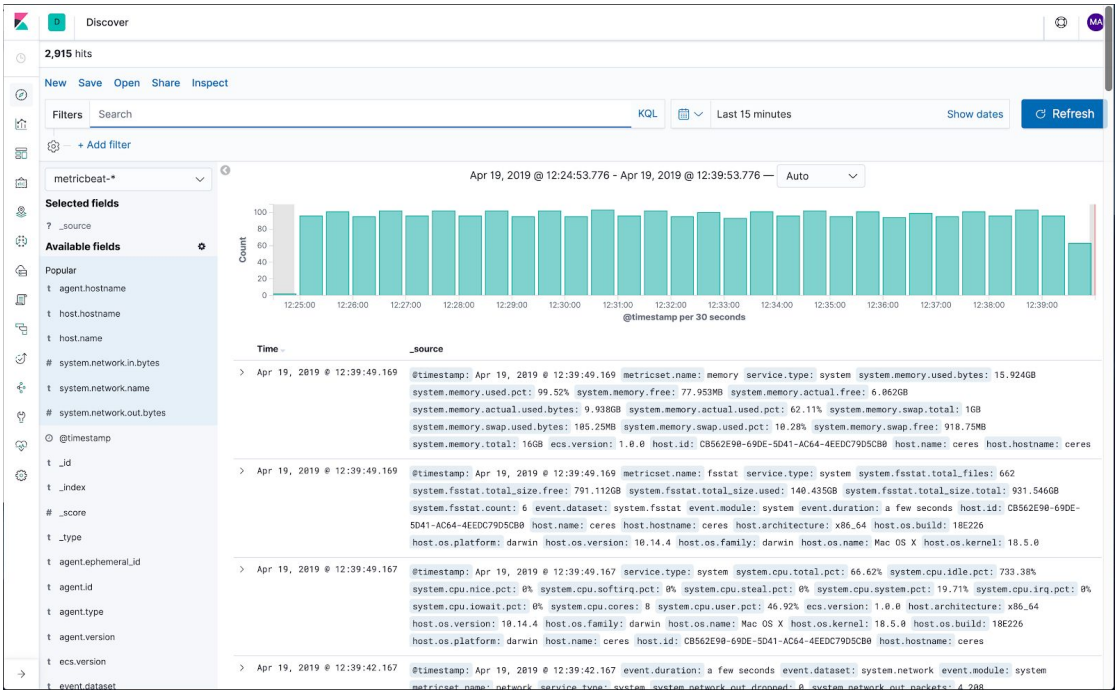
6) Give it a username and a password, full name, and email. In the roles assigned to the user select **`kibana-user`** and **`metrics-admin`**. Click on **`Create User`** button.

Note: Security feature do provide the capabilities to integrate the roles you created into your Security providers with security standards such as SAML based integration (Azure AD, Okta and other SAML Providers). They are outside the scope of the labs.

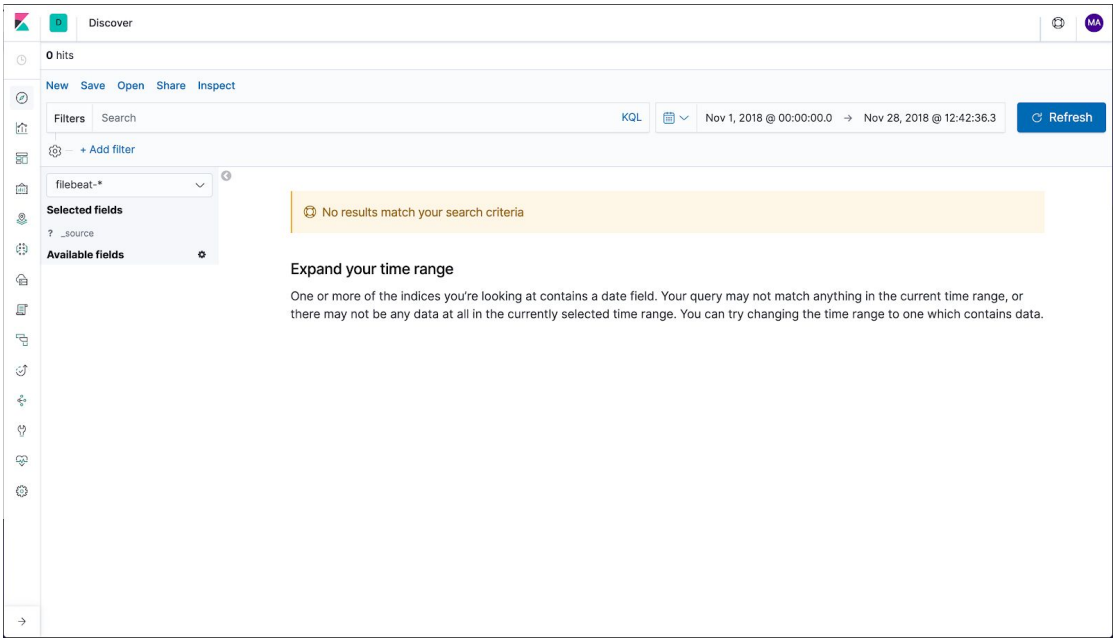


7) From another browser (or same browser incognito/private mode to avoid session mixup) login to that same cluster with the newly created user credentials. Once you login click on **`Discover`** tab on Kibana menu. Note that the only index pattern you can see data for is **`metricbeat-*`** and for **`filebeat-*`** index pattern you cannot see any data even with the correct time range (Nov-01-2018 to Nov-28-2018).

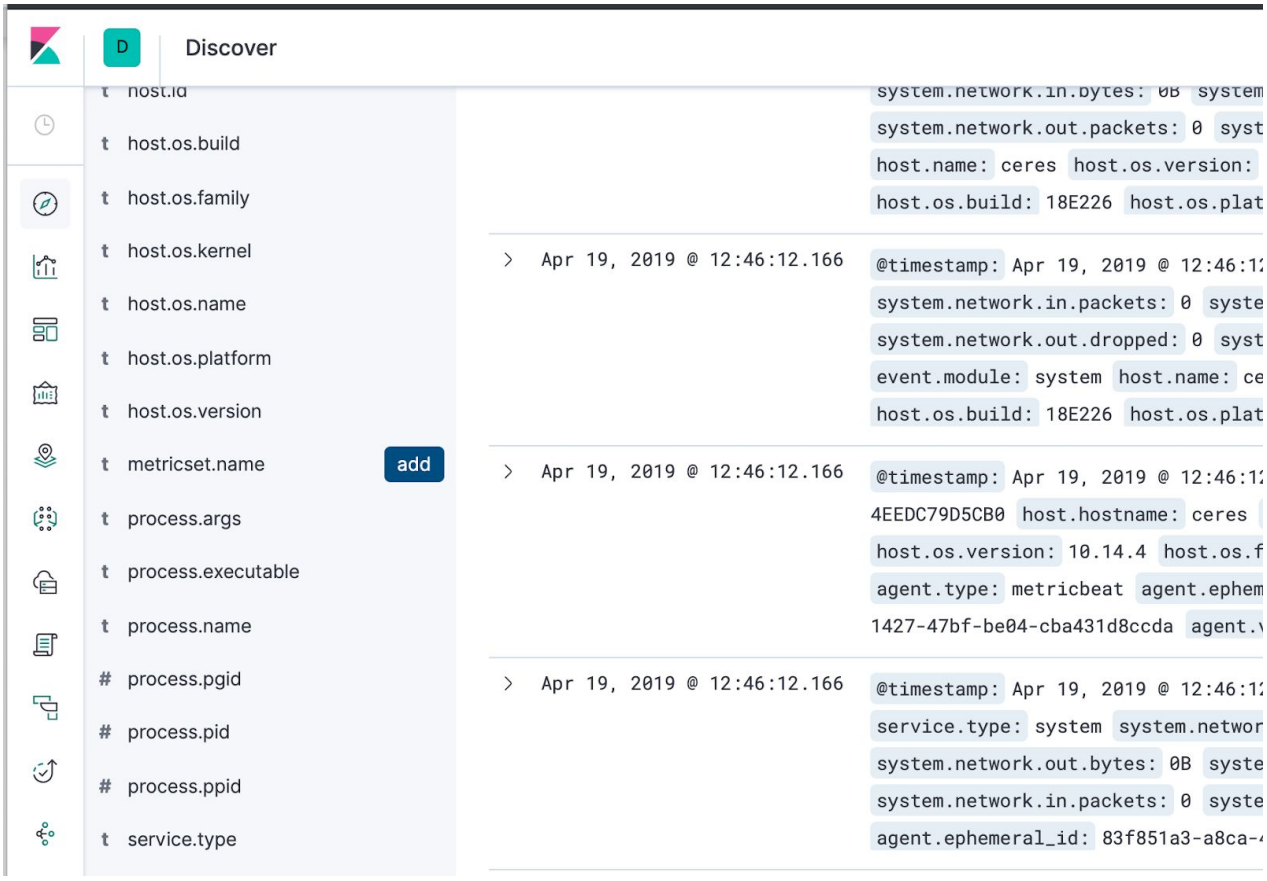
Metricbeat

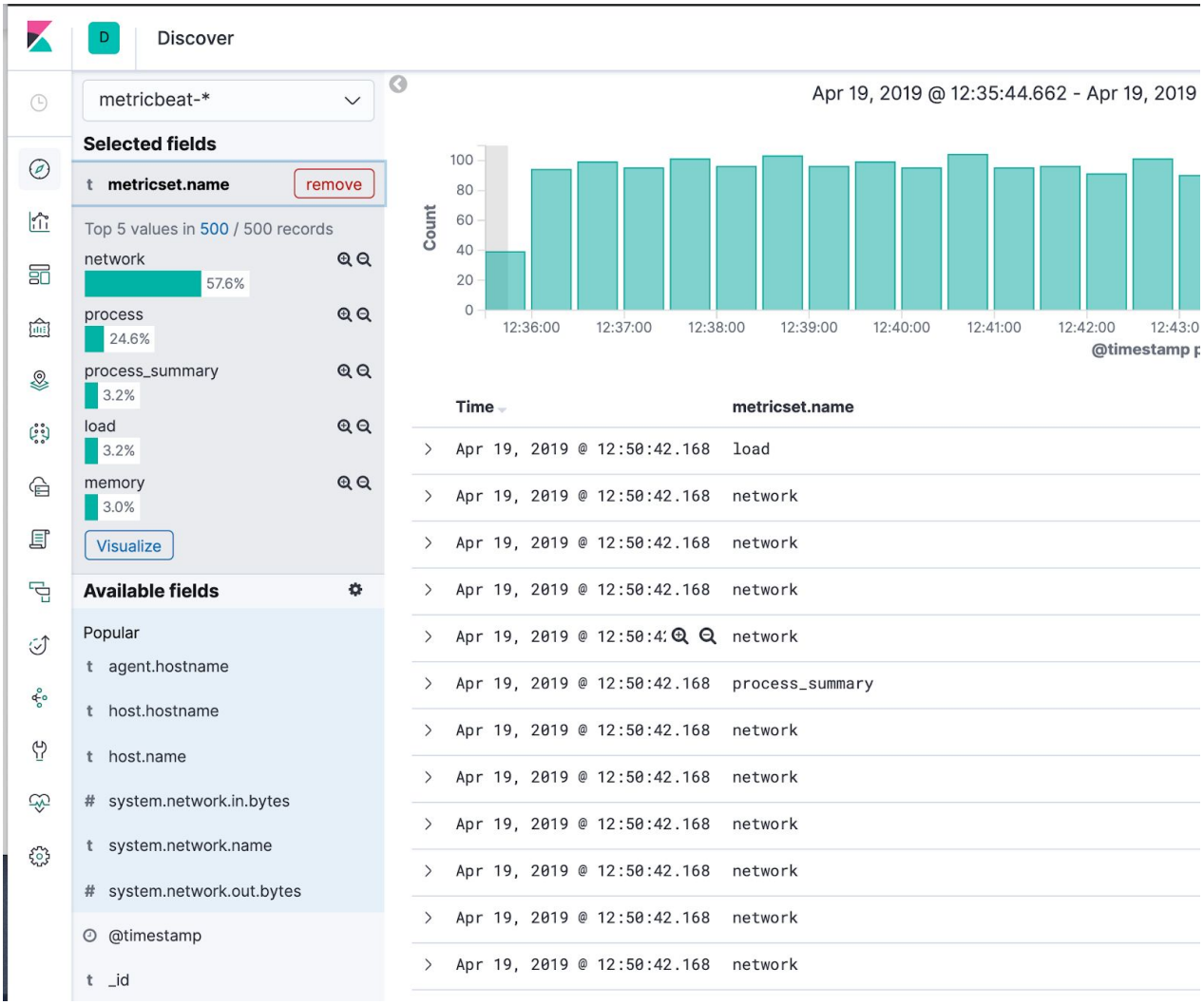


Filebeat



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.

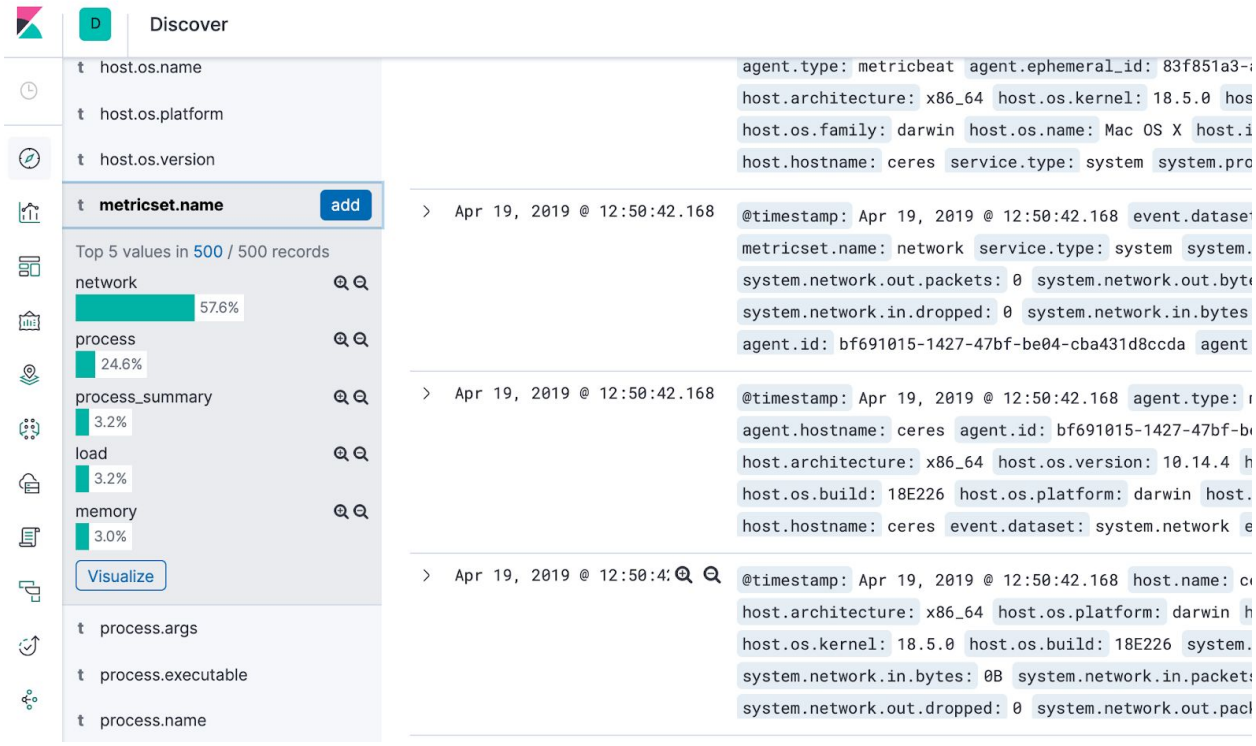

Discover
t host.id
t host.os.build
t host.os.family
t host.os.kernel
t host.os.name
t host.os.platform
t host.os.version
t metricset.name
add
t process.args
t process.executable
t process.name
process.pgid
process.pid
process.ppid
t service.type
system.network.in.bytes: 0B system
system.network.out.packets: 0 syst
host.name: ceres host.os.version:
host.os.build: 18E226 host.os.plat
Apr 19, 2019 @ 12:46:12.166
@timestamp: Apr 19, 2019 @ 12:46:1
system.network.in.packets: 0 syste
system.network.out.dropped: 0 syst
event.module: system host.name: ce
host.os.build: 18E226 host.os.plat
Apr 19, 2019 @ 12:46:12.166
@timestamp: Apr 19, 2019 @ 12:46:1
4EEDC79D5CB0 host.hostname: ceres
host.os.version: 10.14.4 host.os.f
agent.type: metricbeat agent.ephem
1427-47bf-be04-cba431d8ccda agent.
Apr 19, 2019 @ 12:46:12.166
@timestamp: Apr 19, 2019 @ 12:46:1
service.type: system system.networ
system.network.out.bytes: 0B syste
system.network.in.packets: 0 syste
agent.ephemeral_id: 83f851a3-a8ca-



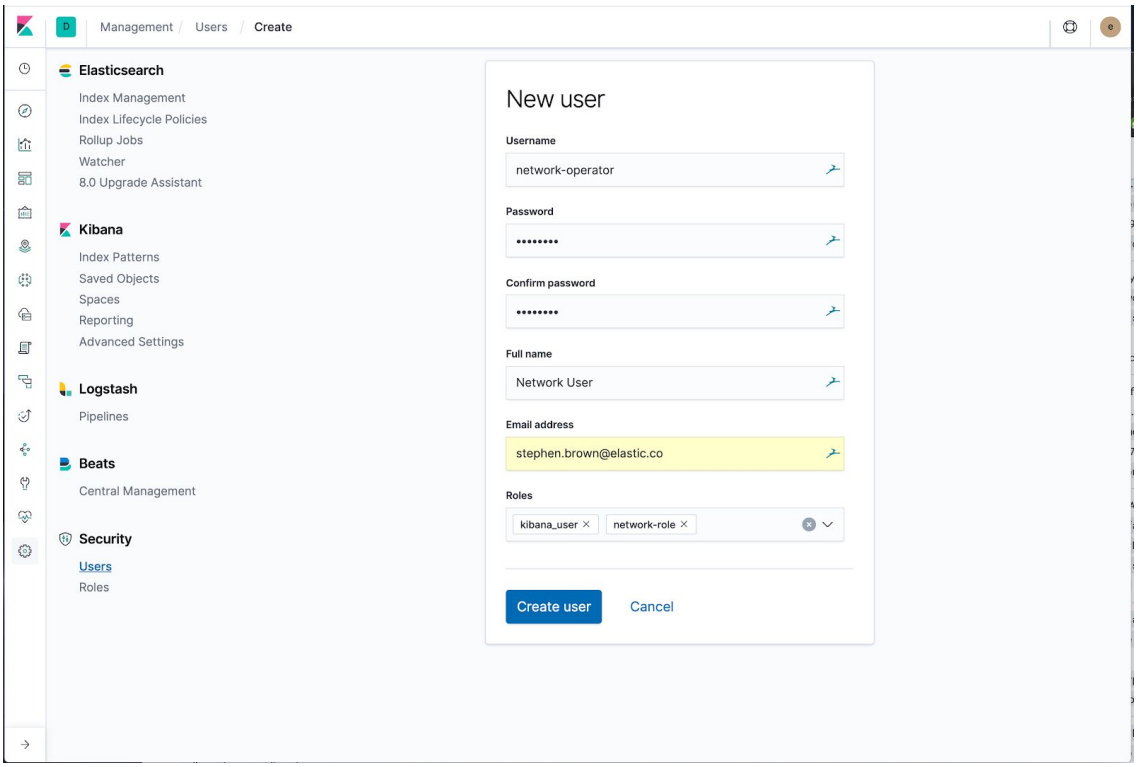
9) One of the data types we are collecting is **`network`**. Imagine a scenario in which we have network operations users that are only allowed to see networking metrics and nothing else from the metrics that were captured. Can we provide them document level access based on this attribute (**`Document 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-role`**.

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"}}`

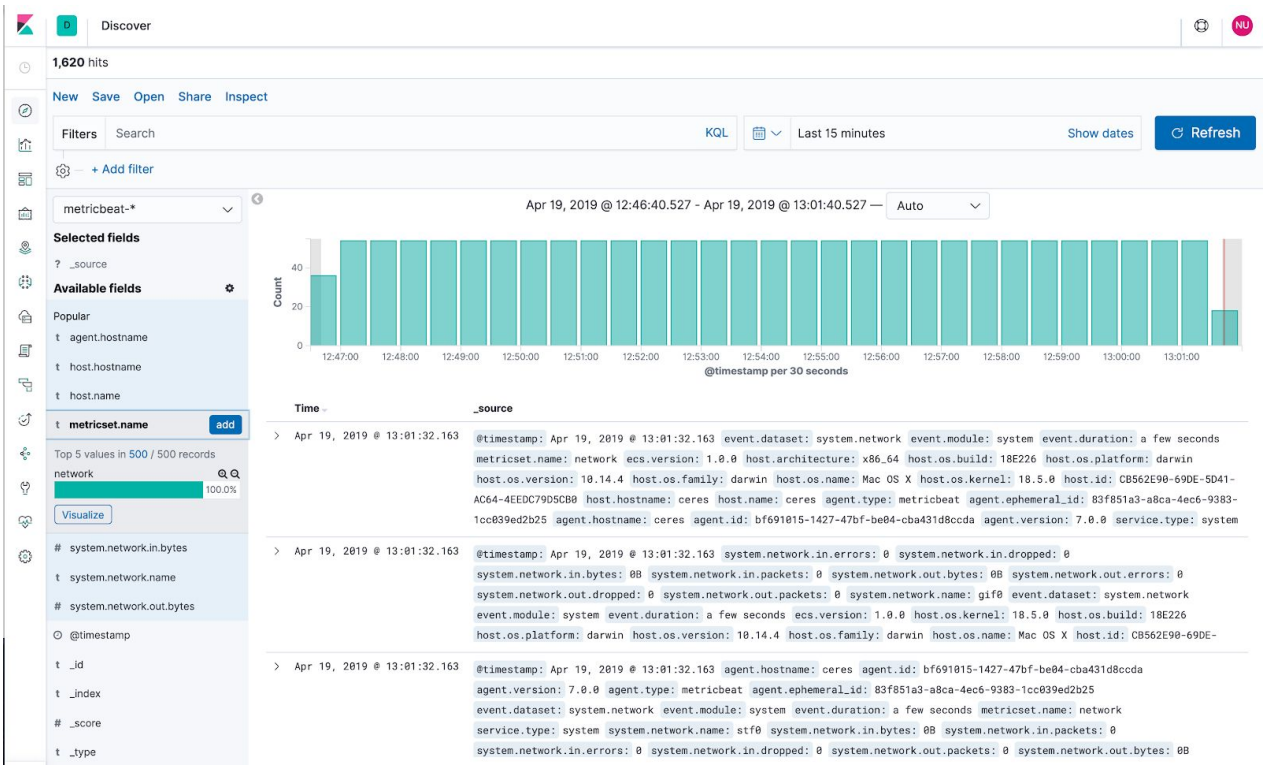
Click on **`Create Role`**.



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.



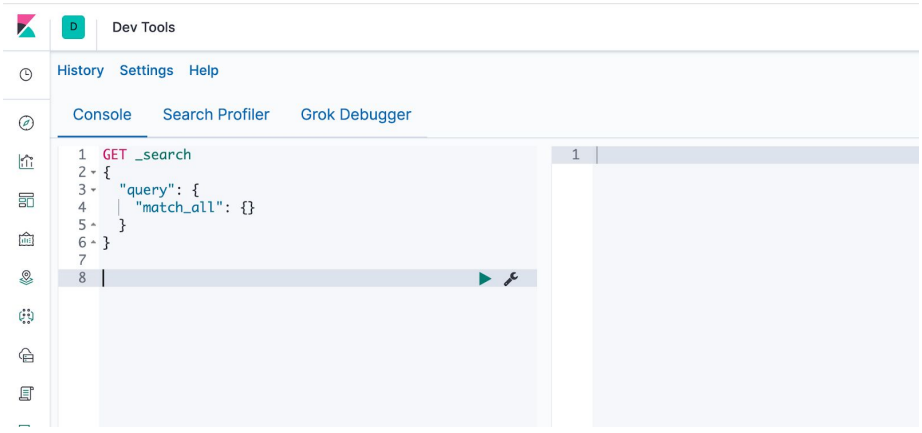
11) Login as this newly created user, click on Discover and select **`metricbeat-*`** index pattern. Expand **`metricset.name`** field by clicking on it and note how the only value visible now is **`network`**. All the other values, that are visible to **`metrics-admin`** are not visible to this user.



12) Let's expand another capability of our Security feature called **Field Level Security**. Login in as elastic user and select **`filebeat-*`** index pattern. Change the dates to be between **`Nov 1st, 2018 and Nov 28th, 2018`**. Click on the fields **`source.ip, source.address`** and **`nginx.access.remote_ip_list`**. These fields display IPs of users who accessed our site. This could be sensitive information that you would like to be available only to admin

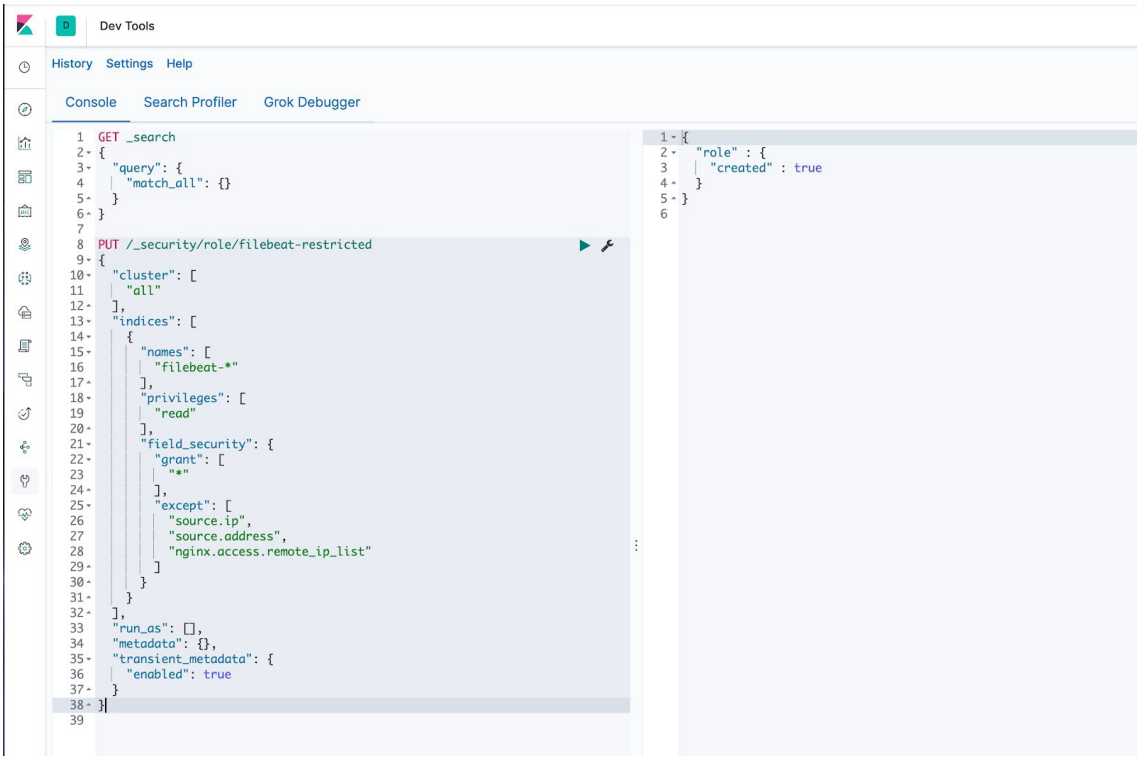
users.

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`** app on the side navigation menu and click **`Get to Work`** and paste the following code snippet into the left window.

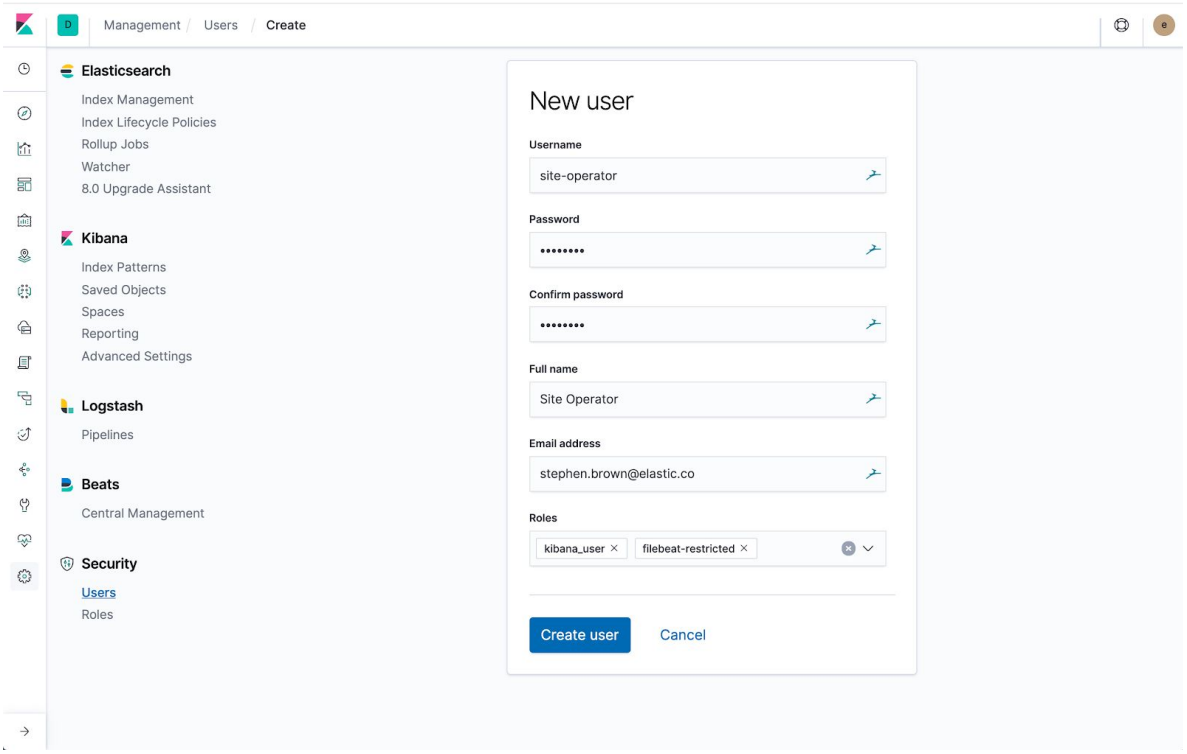


```
PUT /_security/role/filebeat-restricted
{
  "cluster": [
    "all"
  ],
  "indices": [
    {
      "names": [
        "filebeat-*"
      ],
      "privileges": [
        "read"
      ],
      "field_security": {
        "grant": [
          "*"
        ],
        "except": [
          "source.ip",
          "source.address",
          "nginx.access.remote_ip_list"
        ]
      }
    }
  ],
  "run_as": [],
  "metadata": {},
  "transient_metadata": {
    "enabled": true
  }
}
```

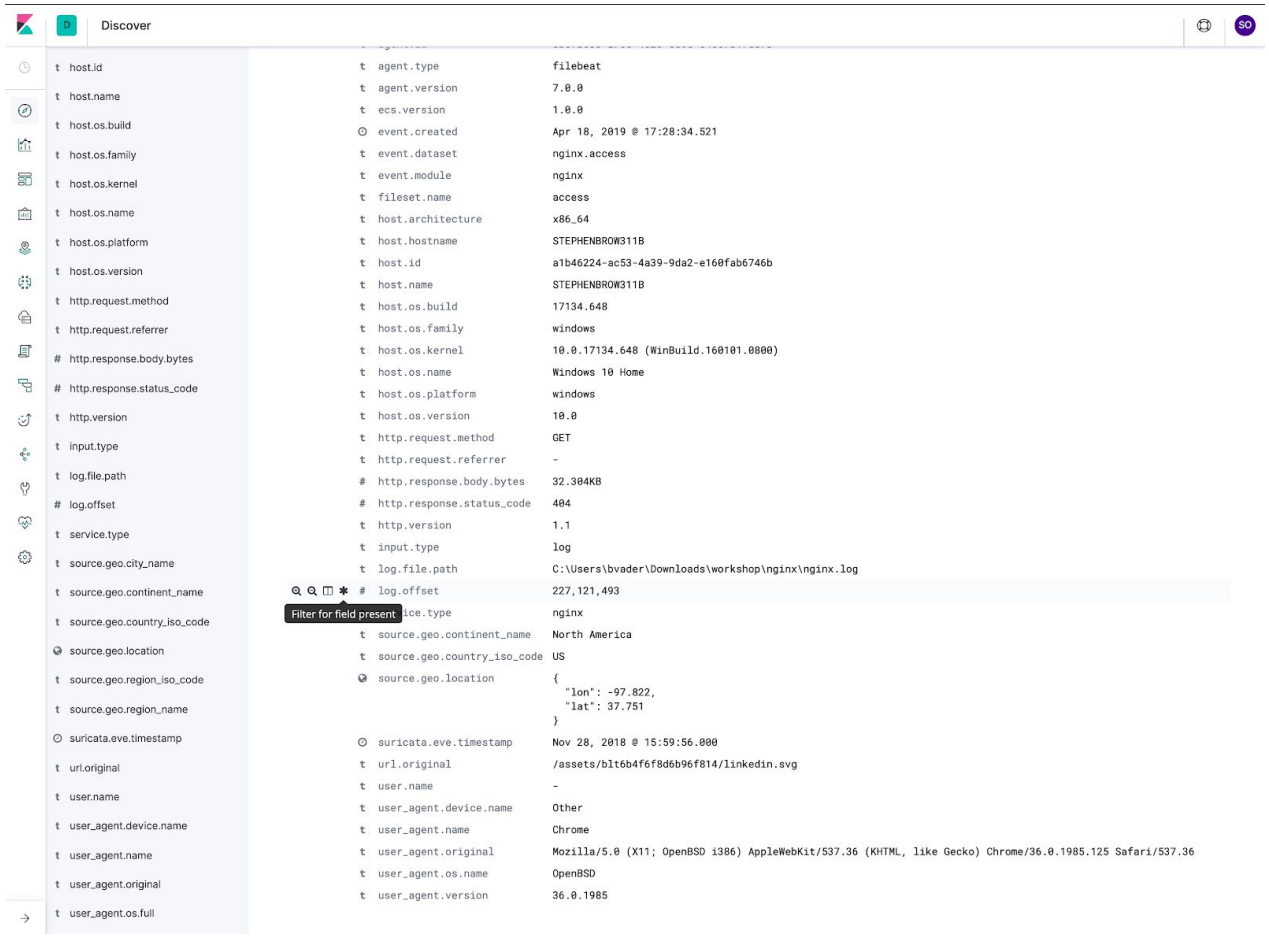
Execute the API call



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



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 learned how to secure sensitive data in the Elasticsearch using ***Index Level***, ***Document Level***, and ***Field Level*** Role Based Access