

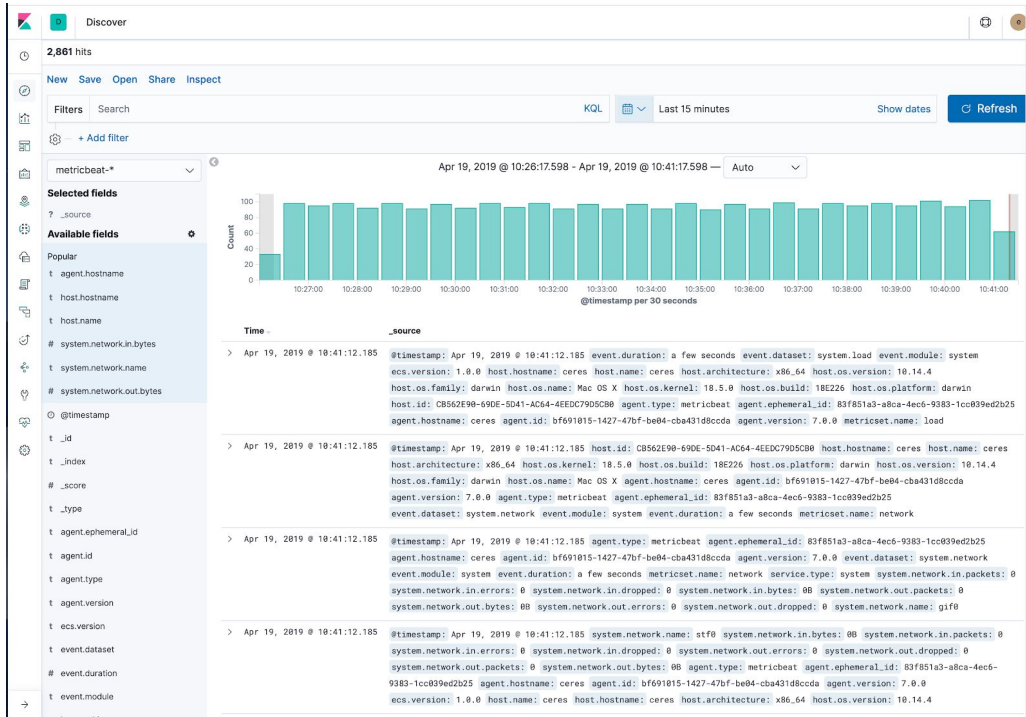


Elastic Observability Workshop

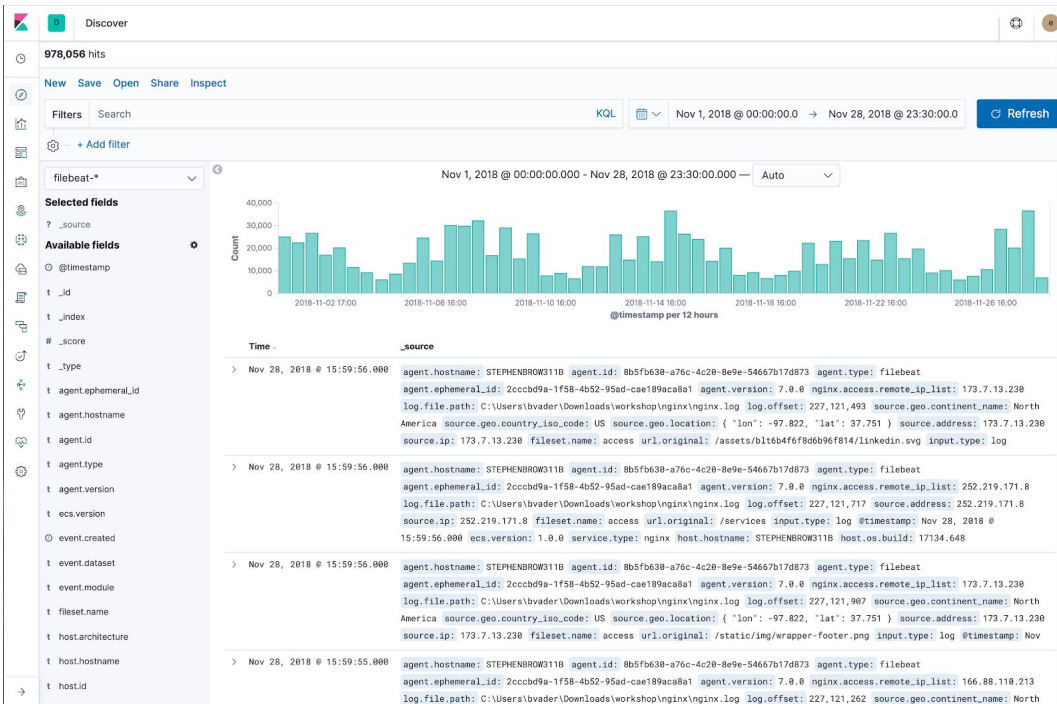
Lab 3 - Security

metricbeat-* index pattern. When selecting **filebeat-*** use date range **Nov 1st, 2018 - Nov 28th, 2018**. When selecting **metricbeat-*** use **Last 15 min.**

Metricbeat

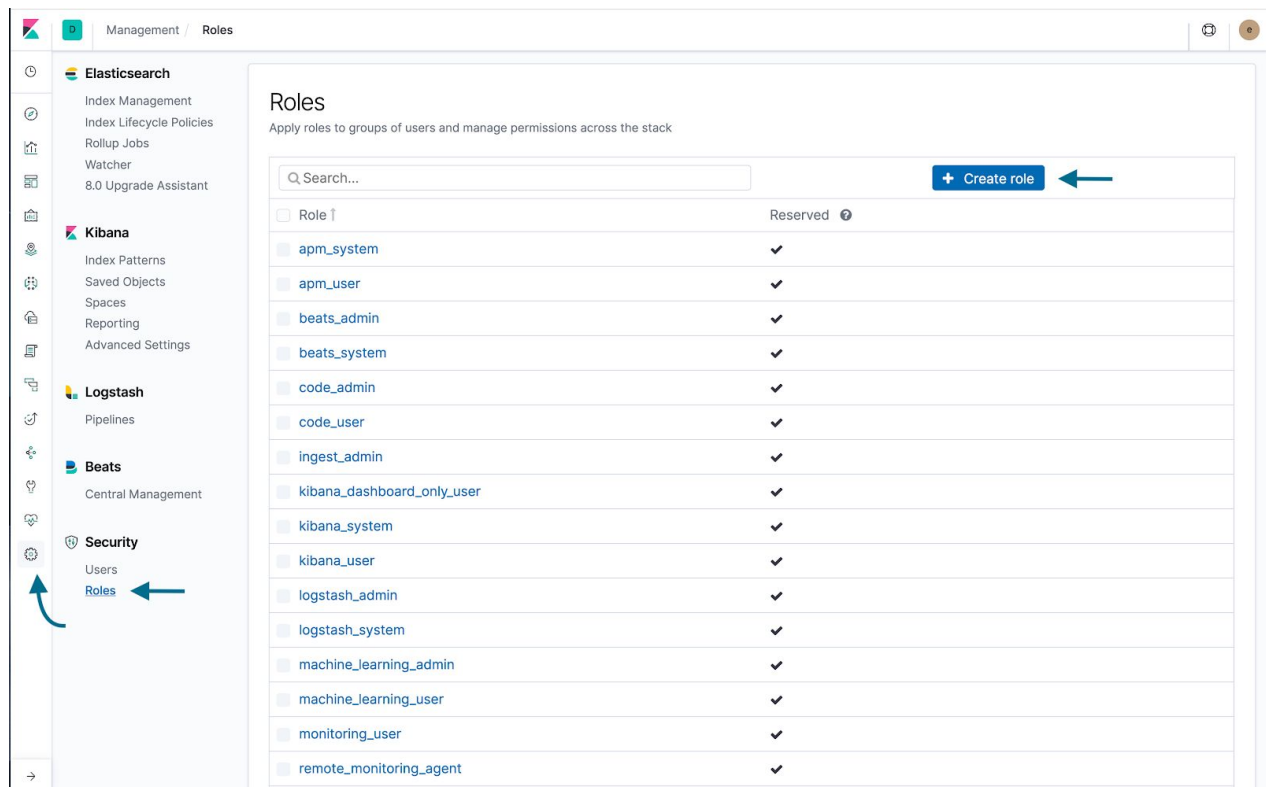


Filebeat



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**

Management / Users / Create

Create role

Set privileges on your Elasticsearch data and control access to your Kibana spaces.

Role name
metrics-admin

Elasticsearch hide

Cluster privileges
Manage the actions this role can perform against your cluster. [Learn more](#)

all x

Run As privileges
Allow requests to be submitted on the behalf of other users. [Learn more](#)

Add a user...

Index privileges
Control access to the data in your cluster. [Learn more](#)

Indices: metricbeat-* x Privileges: all x Granted fields (optional): * x

☐ Grant read privileges to specific documents

[Add index privilege](#)

Kibana hide

Minimum privileges for all spaces
Specify the minimum actions users can perform in your spaces.

none

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**

Management / Users

Users

[Create new user](#)

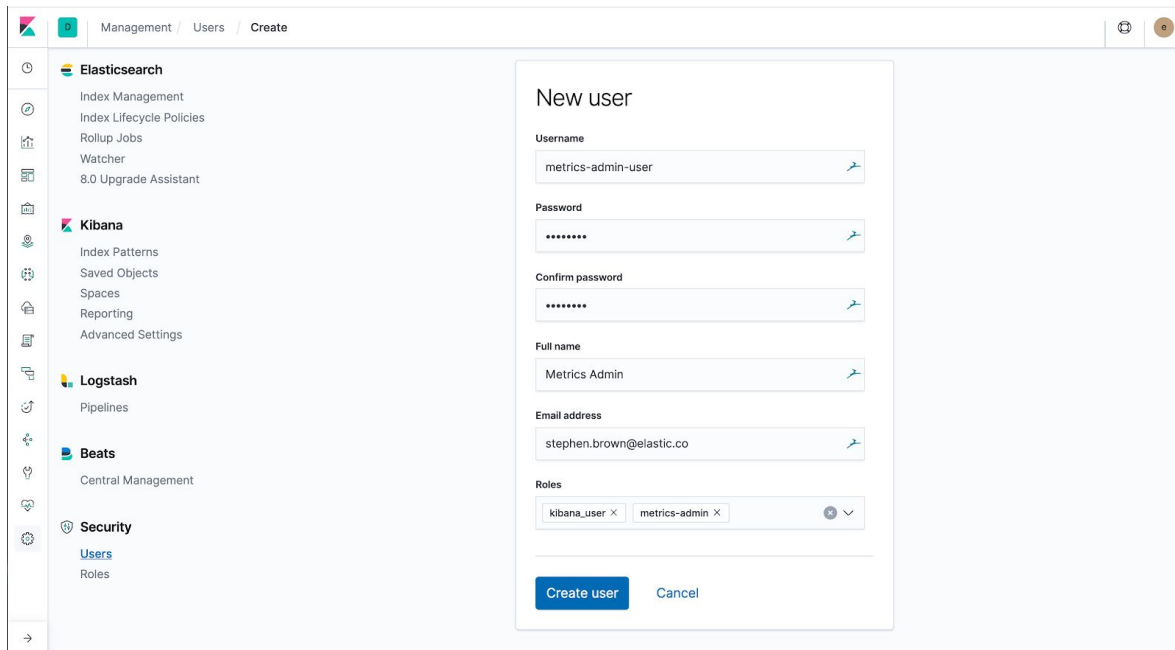
Search...

Full Name ↑	User Name	Email Address	Roles	Reserved
	anonymous		anonymous	✓

Rows per page: 20

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.

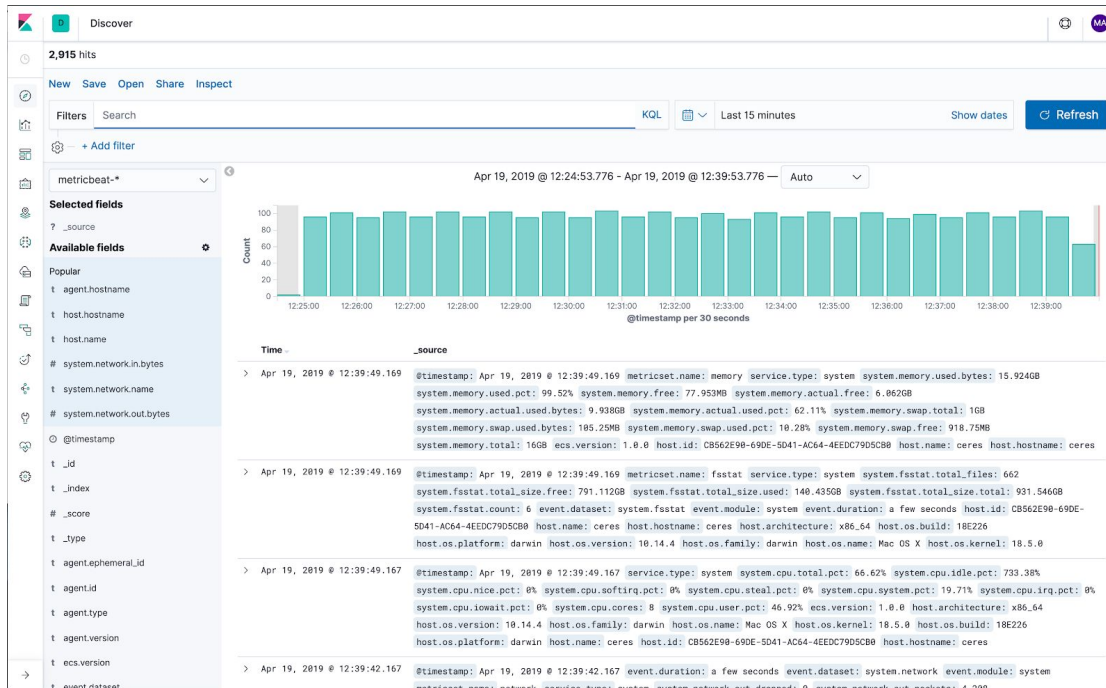
Note: Security feature do provide the capabilities to integrate the roles you created into your Security providers with security standards such as SAML based integration (Azure AD, Okta and other SAML Providers). They are outside the scope of the labs.



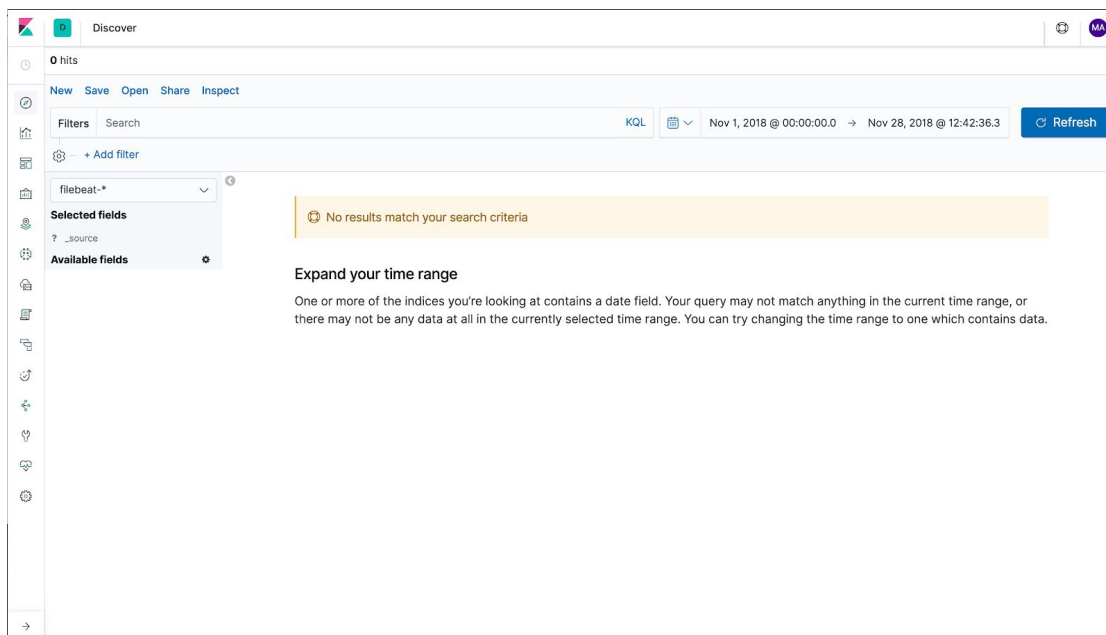
The screenshot shows the Kibana 'New user' creation form. The left sidebar contains a navigation menu with categories: Elasticsearch (Index Management, Index Lifecycle Policies, Rollup Jobs, Watcher, 8.0 Upgrade Assistant), Kibana (Index Patterns, Saved Objects, Spaces, Reporting, Advanced Settings), Logstash (Pipelines), Beats (Central Management), and Security (Users, Roles). The main content area is titled 'New user' and contains the following fields: Username (metrics-admin-user), Password (masked with dots), Confirm password (masked with dots), Full name (Metrics Admin), and Email address (stephen.brown@elastic.co). Below these fields is a 'Roles' section with two selected roles: kibana_user and metrics-admin. At the bottom of the form are two buttons: 'Create user' and 'Cancel'.

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

🕒

🔍

📊

📁

📅

🌐

👤

🔧

📄

🔄

🔗

host.id

host.os.build

host.os.family

host.os.kernel

host.os.name

host.os.platform

host.os.version

metricset.name

process.args

process.executable

process.name

process.pgpid

process.pid

process.ppid

service.type

add

> Apr 19, 2019 @ 12:46:12.166

@timestamp: Apr 19, 2019 @ 12:46:12.166

system.network.in.bytes: 0B

system.network.out.packets: 0

host.name: ceres

host.os.version: 10.14.4

host.os.build: 18E226

host.os.platform: darwin

> Apr 19, 2019 @ 12:46:12.166

@timestamp: Apr 19, 2019 @ 12:46:12.166

4EEDC79D5CB0

host.hostname: ceres

host.os.version: 10.14.4

host.os.family: darwin

agent.type: metricbeat

agent.ephemeral_id: 1427-47bf-be04-cba431d8ccda

agent.type: metricbeat

> Apr 19, 2019 @ 12:46:12.166

@timestamp: Apr 19, 2019 @ 12:46:12.166

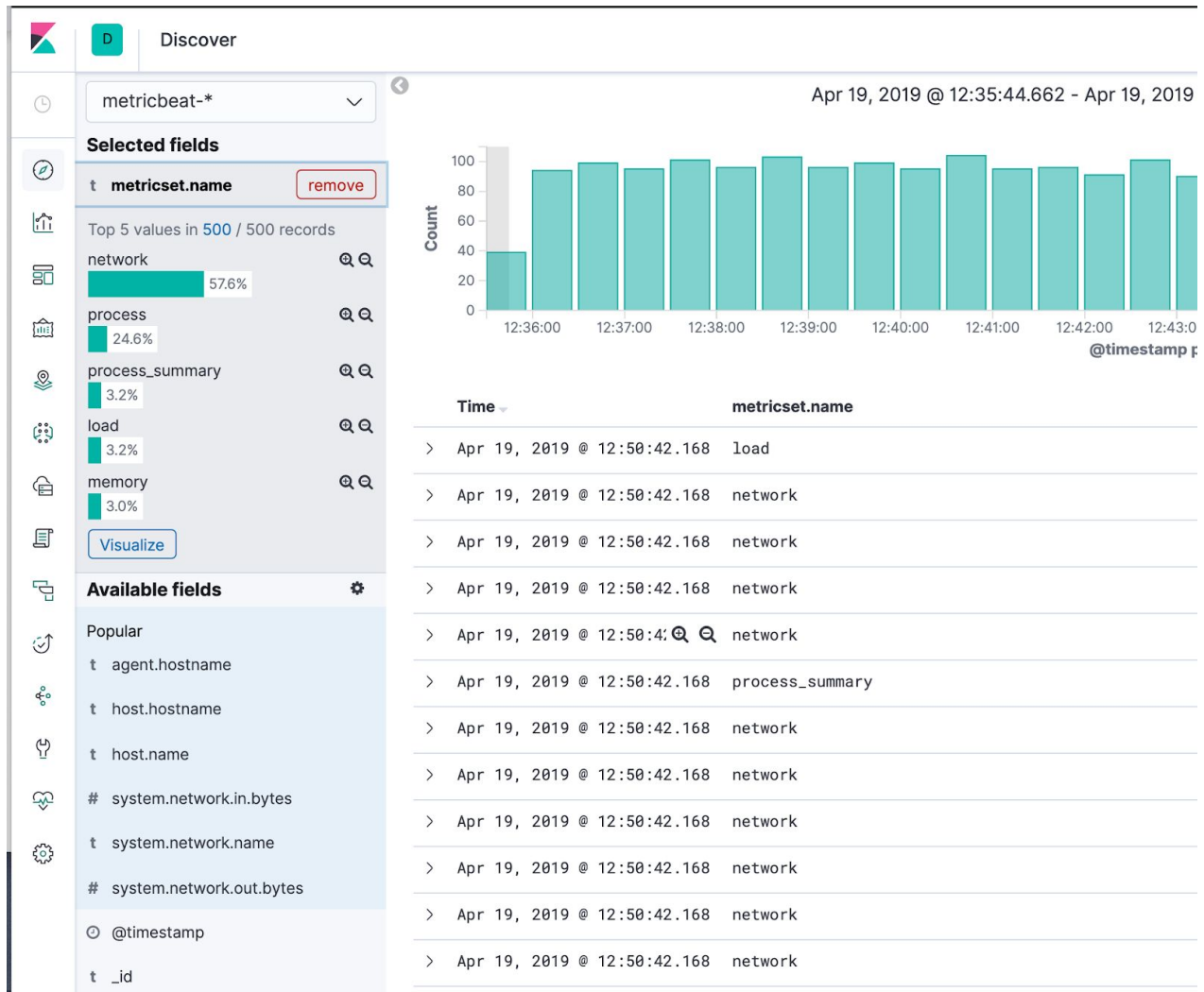
service.type: system

system.network.in.bytes: 0B

system.network.out.packets: 0

system.network.in.packets: 0

agent.ephemeral_id: 83f851a3-a8ca-4



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**.

Discover

host.os.name

host.os.platform

host.os.version

metricset.name

Top 5 values in 500 / 500 records

network

57.6%

process

24.6%

process_summary

3.2%

load

3.2%

memory

3.0%

Visualize

process.args

process.executable

process.name

agent.type: metricbeat agent.ephemeral_id: 83f851a3-i

host.architecture: x86_64 host.os.kernel: 18.5.0 hos

host.os.family: darwin host.os.name: Mac OS X host.i

host.hostname: ceres service.type: system system.pro

Apr 19, 2019 @ 12:50:42.168

@timestamp: Apr 19, 2019 @ 12:50:42.168 event.datase:

metricset.name: network service.type: system system.

system.network.out.packets: 0 system.network.out.byte

system.network.in.dropped: 0 system.network.in.bytes

agent.id: bf691015-1427-47bf-be04-cba431d8ccda agent

Apr 19, 2019 @ 12:50:42.168

@timestamp: Apr 19, 2019 @ 12:50:42.168 agent.type: r

agent.hostname: ceres agent.id: bf691015-1427-47bf-b

host.architecture: x86_64 host.os.version: 10.14.4 h

host.os.build: 18E226 host.os.platform: darwin host.

host.hostname: ceres event.dataset: system.network e

Apr 19, 2019 @ 12:50:42.168

@timestamp: Apr 19, 2019 @ 12:50:42.168 host.name: c

host.architecture: x86_64 host.os.platform: darwin h

host.os.kernel: 18.5.0 host.os.build: 18E226 system.

system.network.in.bytes: 0B system.network.in.packets:

system.network.out.dropped: 0 system.network.out.pac

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.

Management / Users / Create

Elasticsearch

Index Management

Index Lifecycle Policies

Rollup Jobs

Watcher

8.0 Upgrade Assistant

Kibana

Index Patterns

Saved Objects

Spaces

Reporting

Advanced Settings

Logstash

Pipelines

Beats

Central Management

Security

Users

Roles

New user

Username

network-operator

Password

Confirm password

Full name

Network User

Email address

stephen.brown@elastic.co

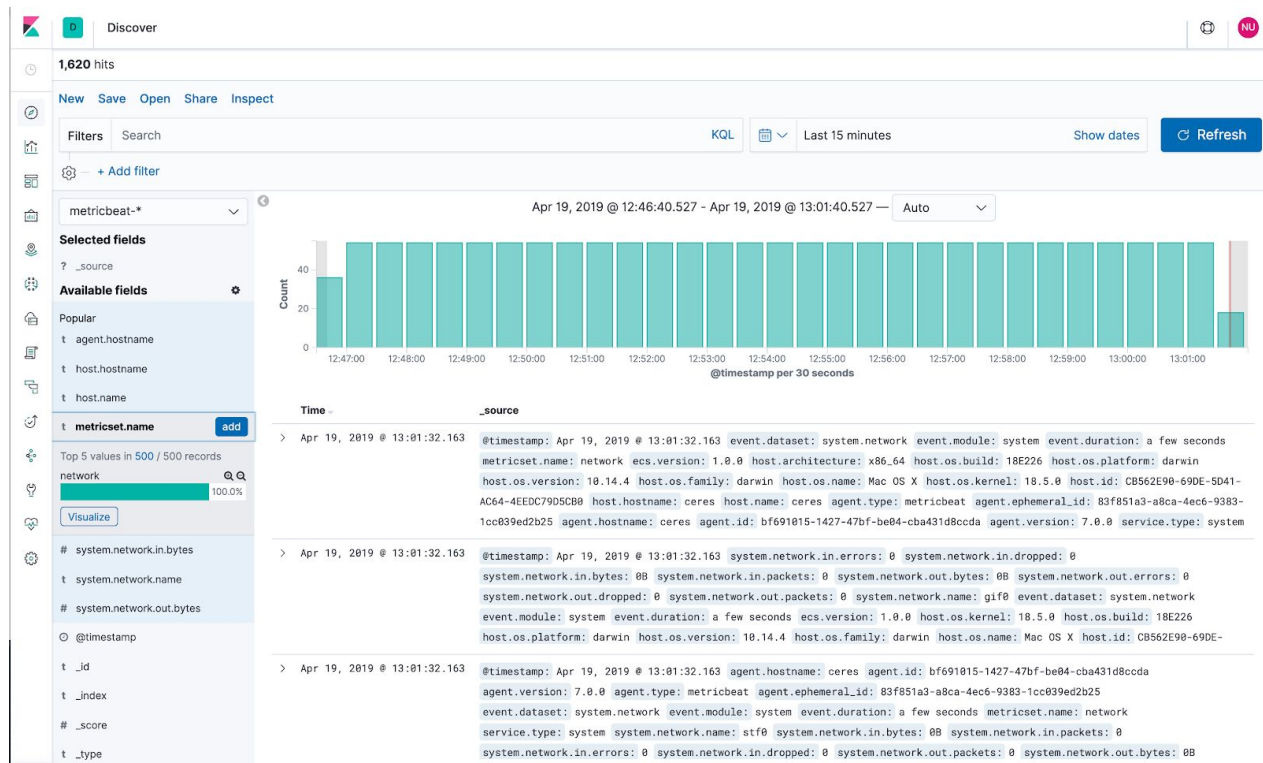
Roles

kibana_user x network-role x

Create user

Cancel

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.

The screenshot shows the Elasticsearch Discover interface. On the left, there's a sidebar with filters and a 'Discover' tab. The main area displays a list of records. The first record is for 'nginx.access.remote_ip_list' with a timestamp of 'Nov 28, 2018 @ 15:59:41.000'. The second record is for 'source.address' with a timestamp of 'Nov 28, 2018 @ 15:59:40.000'. The third record is for 'source.city_name' with a timestamp of 'Nov 28, 2018 @ 15:59:36.000'. The fourth record is for 'source.continent_name' with a timestamp of 'Nov 28, 2018 @ 15:59:36.000'. The fifth record is for 'source.country_iso_code' with a timestamp of 'Nov 28, 2018 @ 15:59:36.000'. The sixth record is for 'source.location' with a timestamp of 'Nov 28, 2018 @ 15:59:36.000'. The seventh record is for 'source.region_iso_code' with a timestamp of 'Nov 28, 2018 @ 15:59:36.000'. The eighth record is for 'source.region_name' with a timestamp of 'Nov 28, 2018 @ 15:59:36.000'. The ninth record is for 'source.ip' with a timestamp of 'Nov 28, 2018 @ 15:59:36.000'. The tenth record is for 'source.ip' with a timestamp of 'Nov 28, 2018 @ 15:59:36.000'. The eleventh record is for 'source.ip' with a timestamp of 'Nov 28, 2018 @ 15:59:36.000'. The twelfth record is for 'source.ip' with a timestamp of 'Nov 28, 2018 @ 15:59:36.000'. The thirteenth record is for 'source.ip' with a timestamp of 'Nov 28, 2018 @ 15:59:36.000'. The fourteenth record is for 'source.ip' with a timestamp of 'Nov 28, 2018 @ 15:59:36.000'. The fifteenth record is for 'source.ip' with a timestamp of 'Nov 28, 2018 @ 15:59:36.000'. The sixteenth record is for 'source.ip' with a timestamp of 'Nov 28, 2018 @ 15:59:36.000'. The seventeenth record is for 'source.ip' with a timestamp of 'Nov 28, 2018 @ 15:59:36.000'. The eighteenth record is for 'source.ip' with a timestamp of 'Nov 28, 2018 @ 15:59:36.000'. The nineteenth record is for 'source.ip' with a timestamp of 'Nov 28, 2018 @ 15:59:36.000'. The twentieth record is for 'source.ip' with a timestamp of 'Nov 28, 2018 @ 15:59:36.000'.

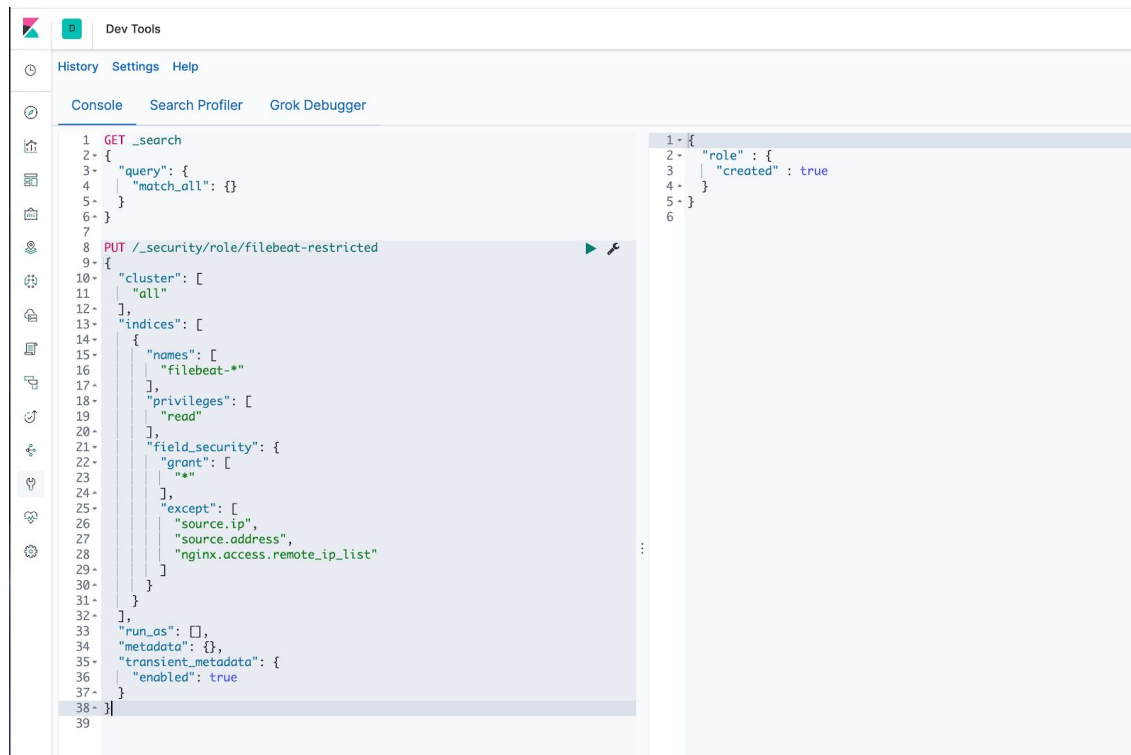
How can we achieve that? Let's create a new role where we would hide this field. But this time let's actually explore API Capabilities of Elasticsearch. Click on **Dev Tools** app on the side navigation menu and click **Get to Work** and paste the following code snippet into the left window.

The screenshot shows the Elasticsearch Dev Tools interface. On the left, there's a sidebar with a 'Dev Tools' tab. The main area displays a console window with a query:

```
1 GET _search
2 {
3   "query": {
4     "match_all": {}
5   }
6 }
7
8
```

```
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
  }
}
```

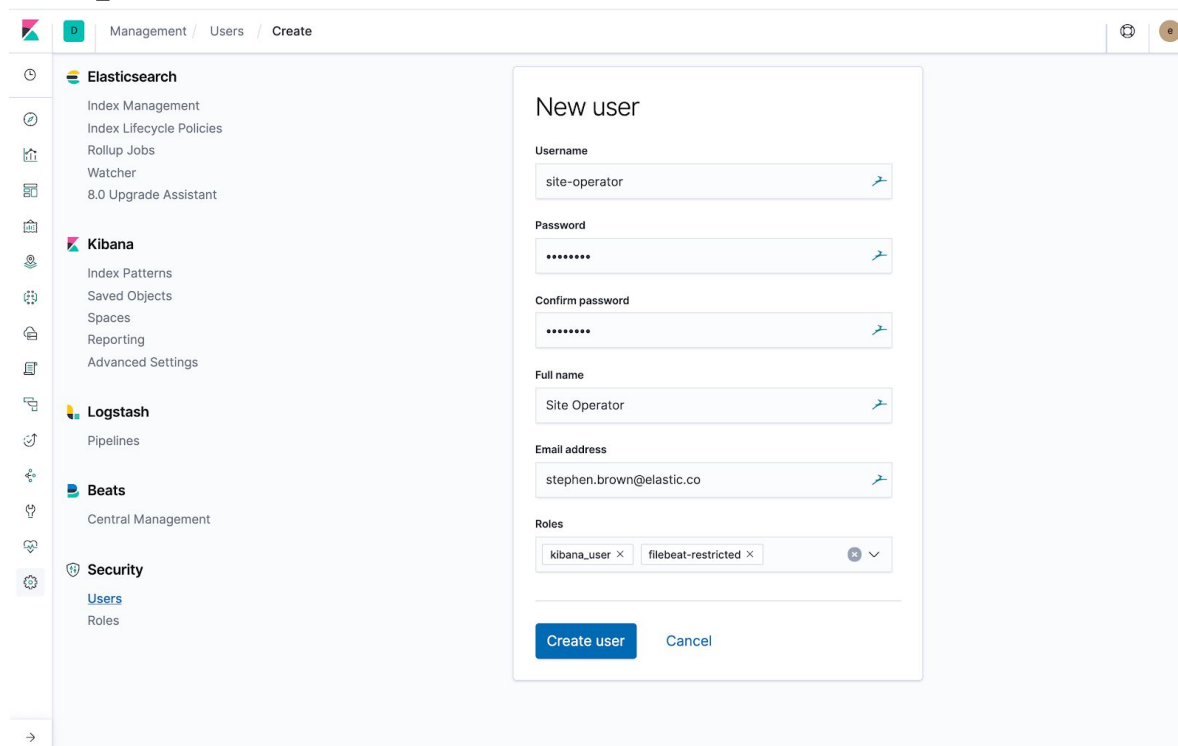
Execute the API call



The screenshot shows the Dev Tools console in a web browser. The left pane displays the console output, and the right pane shows the JSON body of the PUT request. The console output shows a successful response with a 201 status code. The JSON body of the PUT request is as follows:

```
1 GET _search
2 {
3   "query": {
4     "match_all": {}
5   }
6 }
7
8 PUT /_security/role/filebeat-restricted
9 {
10  "cluster": [
11    "all"
12  ],
13  "indices": [
14    {
15      "names": [
16        "filebeat-*"
17      ],
18      "privileges": [
19        "read"
20      ],
21      "field_security": {
22        "grant": [
23          "*"
24        ],
25        "except": [
26          "source.ip",
27          "source.address",
28          "nginx.access.remote_ip_list"
29        ]
30      }
31    }
32  ],
33  "run_as": [],
34  "metadata": {},
35  "transient_metadata": {
36    "enabled": true
37  }
38 }
39
```

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



The screenshot shows the Kibana 'New user' form. The form is titled 'New user' and contains the following fields:

- Username: site-operator
- Password: (masked with dots)
- Confirm password: (masked with dots)
- Full name: Site Operator
- Email address: stephen.brown@elastic.co
- Roles: kibana_user, filebeat-restricted

The 'Roles' field is a dropdown menu with a search icon and a close button. The 'Create user' button is highlighted in blue.

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.

The screenshot shows the Elasticsearch Discover interface. On the left, there is a list of fields. On the right, there is a document view showing the details of a specific document. The document view shows fields like agent.type, agent.version, ecs.version, event.created, event.dataset, event.module, fileset.name, host.architecture, host.hostname, host.id, host.name, host.os.build, host.os.family, host.os.kernel, host.os.name, host.os.platform, host.os.version, http.request.method, http.request.referrer, http.response.body.bytes, http.response.status_code, http.version, input.type, log.file.path, log.offset, service.type, source.geo.city_name, source.geo.continent_name, source.geo.country_iso_code, source.geo.location, source.geo.region_iso_code, source.geo.region_name, suricata.eve.timestamp, url.original, user.name, user_agent.device.name, user_agent.name, user_agent.original, user_agent.os.name, user_agent.os.full, user_agent.version.

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