Kibana logs Exercise

Main goal

The exercise is aimed to get the basic skills in the Elasticsearch configuration. At the end all the students would connect the Elasticsearch environment for getting the logs out of the Kubernetes environment and manipulate them using Kibana visualization.

Initial state

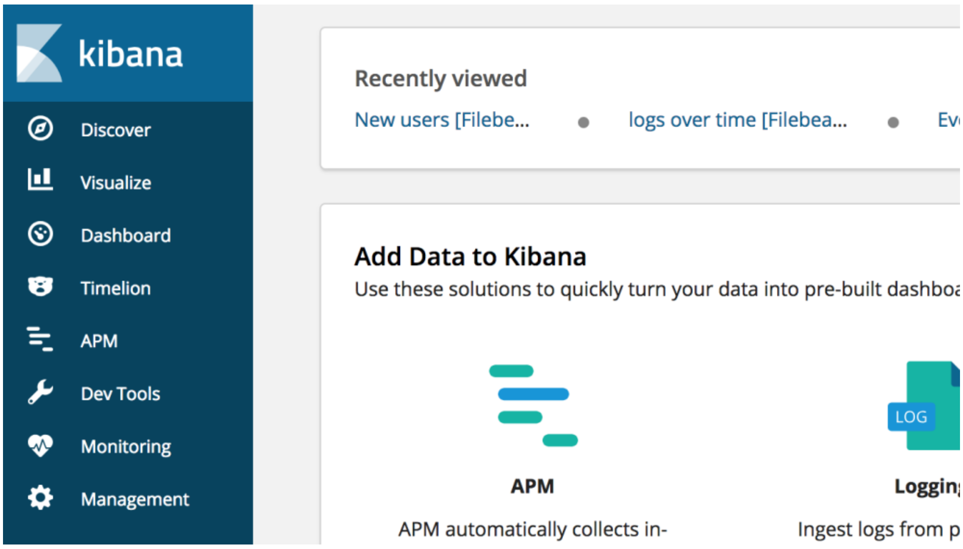
Every student is supplied with the credentials for the virtual course PC and could reach it via HTTP + SSH:

- Jenkins CI server
- K8S master node

Preliminary items

1. Get to the course Jenkins environment using the following credentials:

   http://<your Jenkins PC IP>:8088/



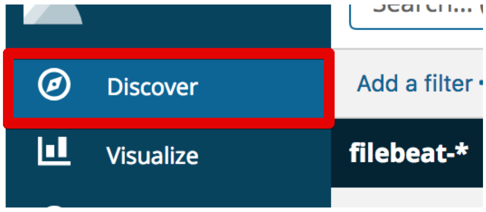
Add Data to Kibana

Use these solutions to quickly turn your data into pre-built dashboa

APM automatically collects in-

Ingest logs from p

2. See the CI server logs:



Configure the k8s server to send logs to the Elasticsearch:

1. Getting the appropriate template to proceed:
   - Go to the K8S master via the SSH and run the following commands:

```
cd ~
curl -L -O
https://raw.githubusercontent.com/elastic/beats/6.4/deploy/kubernetes/filebeat-kubernetes.yaml
```

2. Configuring the template to work with the Elasticsearch host:
   - Open the **filebeat-kubernetes.yaml** and modify the existed line

```
vi filebeat-kubernetes.yaml
```

```
...
env:
        - name: ELASTICSEARCH_HOST
          value: "<YOUR_JENKINS_IP>"
        - name: ELASTICSEARCH_PORT
          value: "9200"
        - name: ELASTICSEARCH_USERNAME
          value: elastic
        - name: ELASTICSEARCH_PASSWORD
         value: changeme
…
```

3. Create the Filebeat instances:

   - Run the command to create the kubernetes items:

```
kubectl create -f filebeat-kubernetes.yaml
```

   - Check the daemon set:

```
kubectl --namespace=kube-system get ds/filebeat
```

Testing the K8S Filebeat Elasticsearch solution:

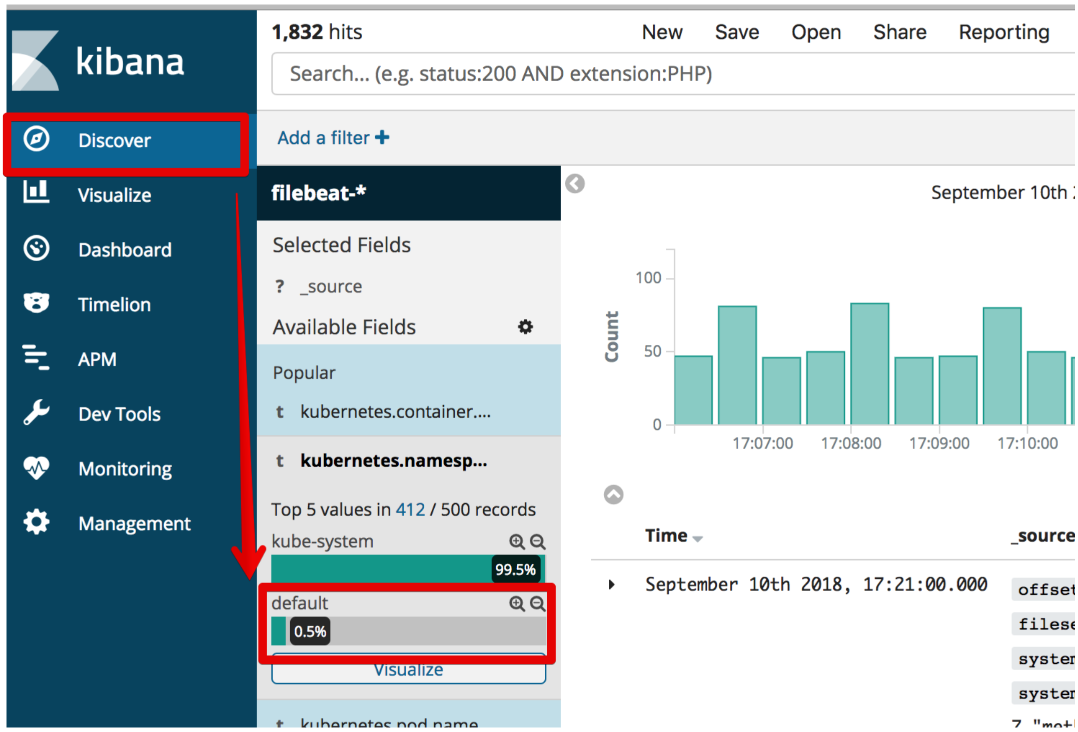
1. Restart the persisted pods from the default namespace:
   - On the K8S master please do the commands:

     kubectl get pods -n default

   - Delete the persisted nexus pod:

     kubectl delete pod < ***-sonatype-nexus-> -n default***

2. Go to Kibana and see the logs from default namespace:

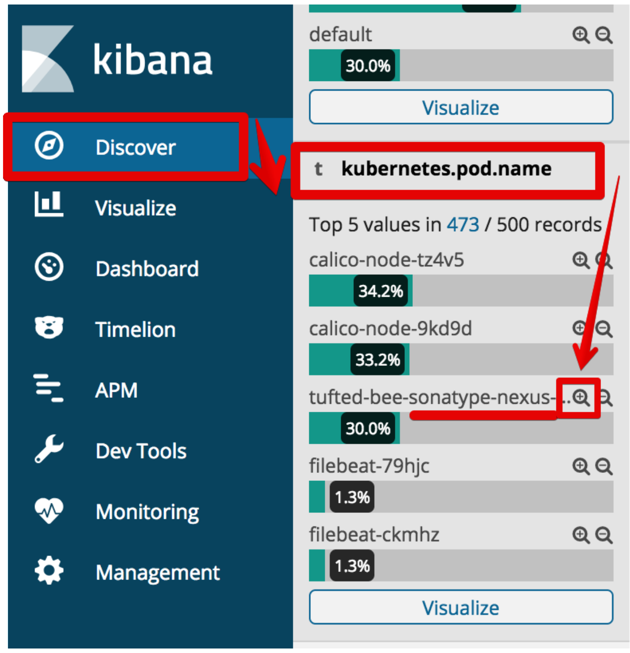


1,832 hits

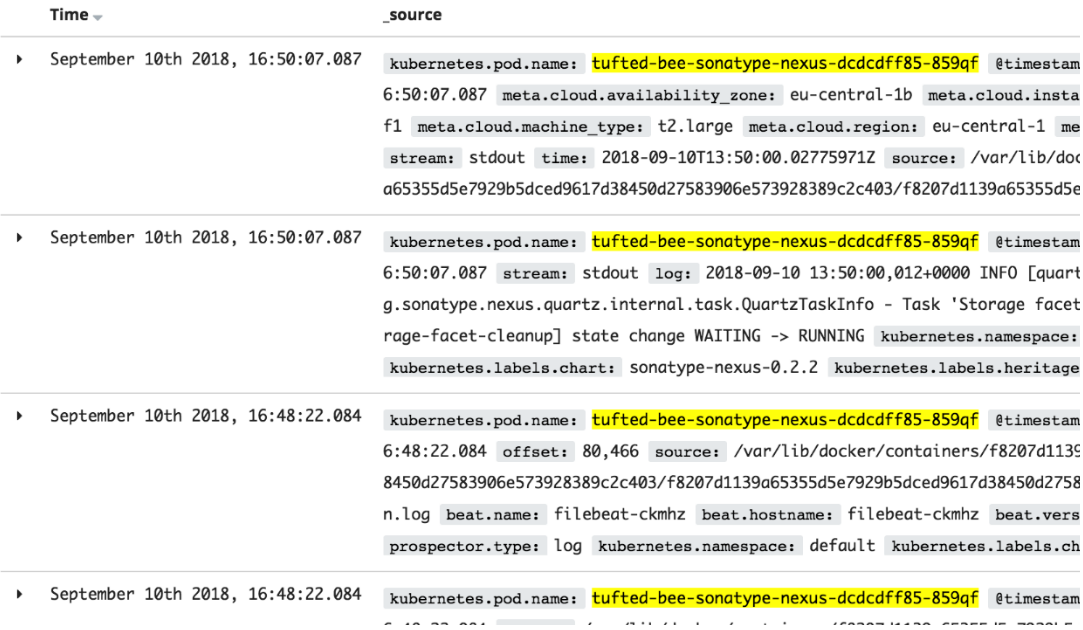
September 10th 2018, 17:21:00.000

© All rights reserved to John Bryce Training LTD from Matrix group

3. Drill down the pod.name:



4. See the related logs:



```
Time          _source

September 10th 2018, 16:50:07.087   kubernetes.pod.name: tufted-bee-sonatype-nexus-dcdcdff85-859qf @timestam
                                    6:50:07.087 meta.cloud.availability_zone: eu-central-1b meta.cloud.insta
                                    f1 meta.cloud.machine_type: t2.large meta.cloud.region: eu-central-1 me
                                    stream: stdout time: 2018-09-10T13:50:00.02775971Z source: /var/lib/doc
                                    a65355d5e7929b5dced9617d38450d27583906e573928389c2c403/f8207d1139a65355d5e

September 10th 2018, 16:50:07.087   kubernetes.pod.name: tufted-bee-sonatype-nexus-dcdcdff85-859qf @timestam
                                    6:50:07.087 stream: stdout log: 2018-09-10 13:50:00,012+0000 INFO [quart
                                    g.sonatype.nexus.quartz.internal.task.QuartzTaskInfo - Task 'Storage facet
                                    rage-facet-cleanup] state change WAITING -> RUNNING kubernetes.namespace:
                                    kubernetes.labels.chart: sonatype-nexus-0.2.2 kubernetes.labels.heritage

September 10th 2018, 16:48:22.084   kubernetes.pod.name: tufted-bee-sonatype-nexus-dcdcdff85-859qf @timestam
                                    6:48:22.084 offset: 80,466 source: /var/lib/docker/containers/f8207d1139
                                    8450d27583906e573928389c2c403/f8207d1139a65355d5e7929b5dced9617d38450d2758
                                    n.log beat.name: filebeat-ckmhz beat.hostname: filebeat-ckmhz beat.vers
                                    prospector.type: log kubernetes.namespace: default kubernetes.labels.ch

September 10th 2018, 16:48:22.084   kubernetes.pod.name: tufted-bee-sonatype-nexus-dcdcdff85-859qf @timestam
```