Cài đặt hệ thống logging tập trung
sử dụng EFK (Elasticsearch Fluentd Kibana)

Author: trantiendt9@gmail.com

Clone bài lab:

Git clone https://github.com/trantiendt9/tranning-devops.git

1. Cài đặt Elasticsearch

Huong dan install helm chart elastic-search

ref https://artifacthub.io/packages/helm/elastic/elasticsearch

1.Tao new namesapce

kubectl create namespace logging-efk

kubectl get ns

2. Download helm chart elastic

helm repo add elastic https://helm.elastic.co

helm repo update

helm search repo elastic --version 7

helm pull elastic/elasticsearch --version 7.17.3

3. Giai nen chart

tar -xvzf elasticsearch-7.17.3.tgz

4. Customize chart

cp elasticsearch/values.yaml values-customize.yaml

5. Install or upgrade helm chart / apply helm chart to K8S cluster

#chart from internet

helm upgrade -i elasticsearch -n logging-efk -f values-customize.yaml elastic/elasticsearch

#chart from already download and extract

helm upgrade -i elasticsearch -n logging-efk -f values-customize.yaml elasticsearch

#kiem tra ket qua:

helm ls -n logging-efk

kubectl get all -n logging-efk

kubectl get svc n logging-efk

2. Cài đặt Fluentd

Huong dan install helm chart fluentd

1.Tao new namesapce

kubectl create namespace logging-efk

kubectl get ns

2. Download helm chart fluentd

helm repo add kokuwa https://kokuwaio.github.io/helm-charts

helm search repo fluentd

helm pull kokuwa/fluentd-elasticsearch --version 11.15.0

3. Giai nen chart

tar -xvzf fluentd-elasticsearch-11.15.0.tgz

4. Customize chart

cp fluentd-elasticsearch/values.yaml values-customize.yaml

#chart from internet

helm upgrade -i fluentd -n logging-efk -f values-customize.yaml stable/fluentd-elasticsearch

#chart from already download and extract

helm upgrade -i fluentd -n logging-efk -f values-customize.yaml fluentd-elasticsearch

#kiem tra ket qua:

helm ls -n logging-efk

kubectl get all -n logging-efk

6. Helm delete/ uninstall chart from K8s Cluster

helm uninstall fluentd -n logging-efk

3. Cài đặt Kibana

Huong dan install helm chart kibana

1.Tao new namesapce

kubectl create namespace logging-efk

kubectl get ns

2. Download helm chart elastic

helm repo add elastic https://helm.elastic.co

helm repo update

helm search repo kibana --version 7

helm pull elastic/kibana --version 7.17.3

3. Giai nen chart

tar -xvzf kibana-7.17.3.tgz

4. Customize chart

cp kibana/values.yaml values-customize.yaml

5. Install or upgrade helm chart / apply helm chart to K8S cluster

#chart from internet

helm upgrade -i kibana -n logging-efk -f values-customize.yaml elastic/kibana

#chart from already download and extract

helm upgrade -i kibana -n logging-efk -f values-customize.yaml kibana

#kiem tra ket qua:

helm ls -n logging-efk

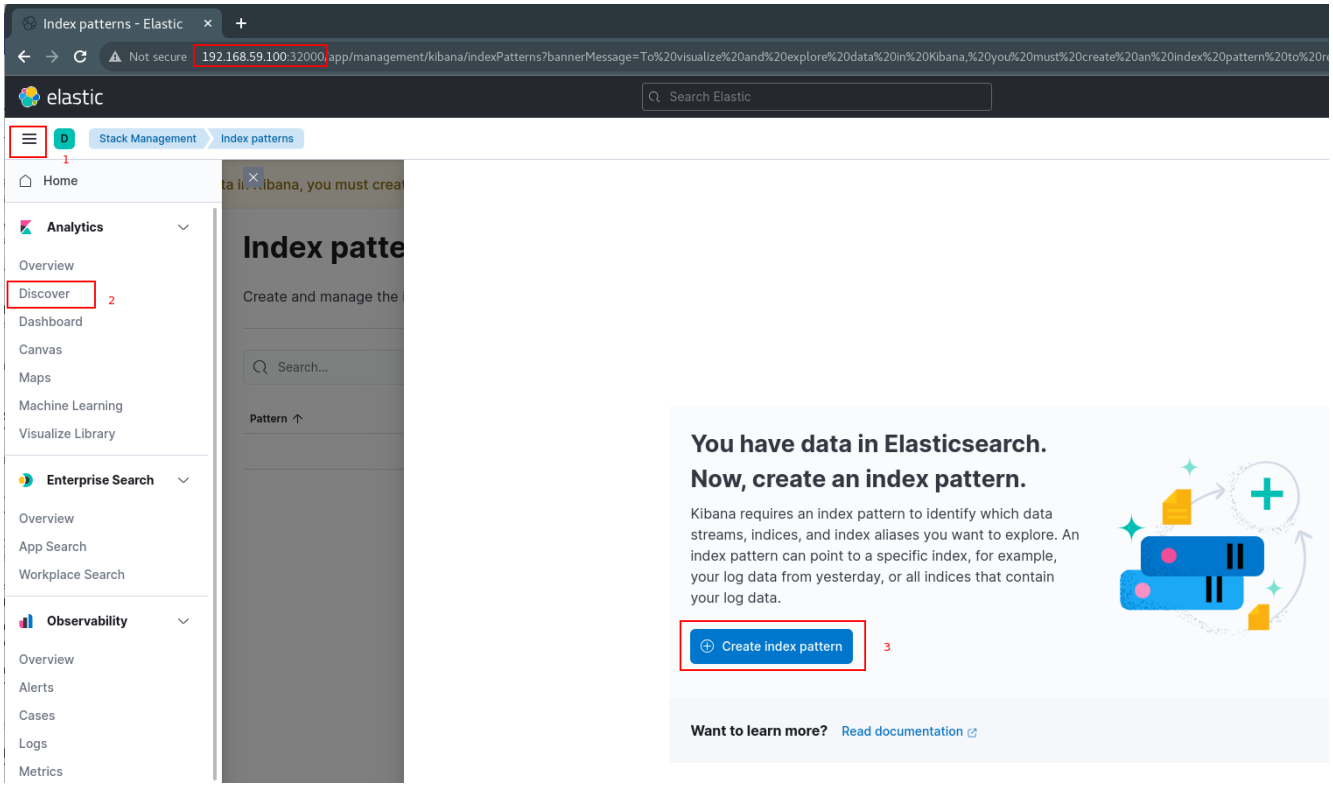
kubectl get all -n logging-efk

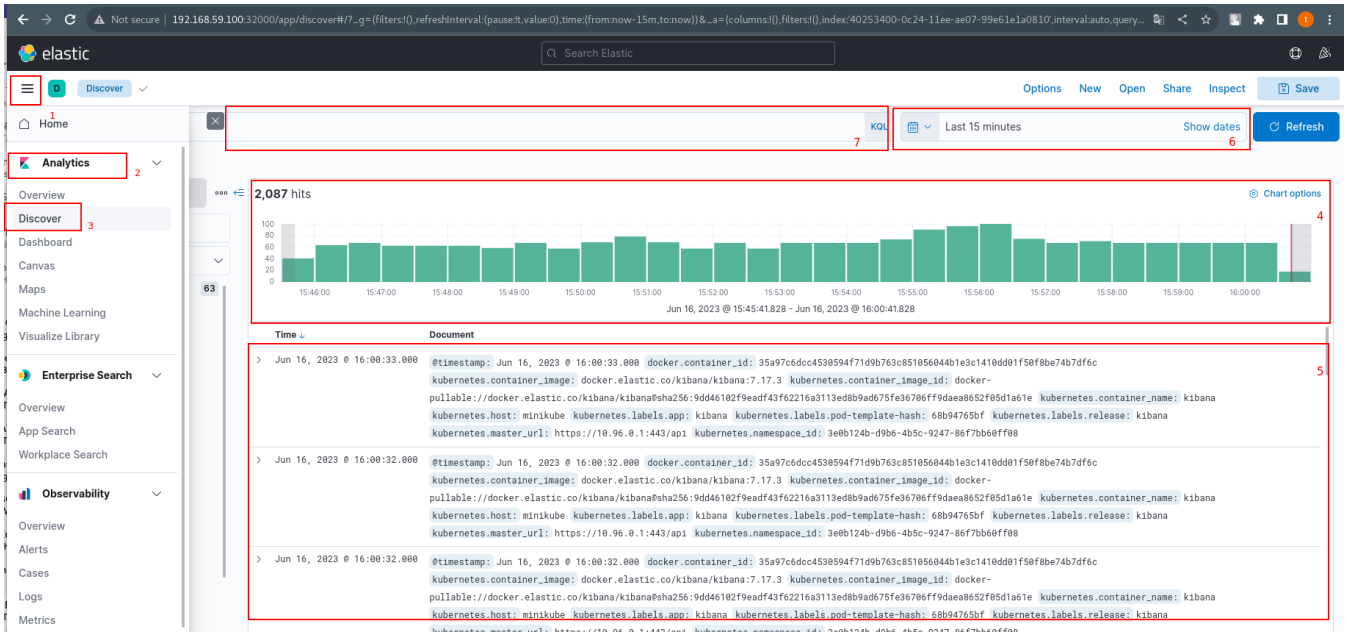
6. Helm uninstall chart from K8s Cluster

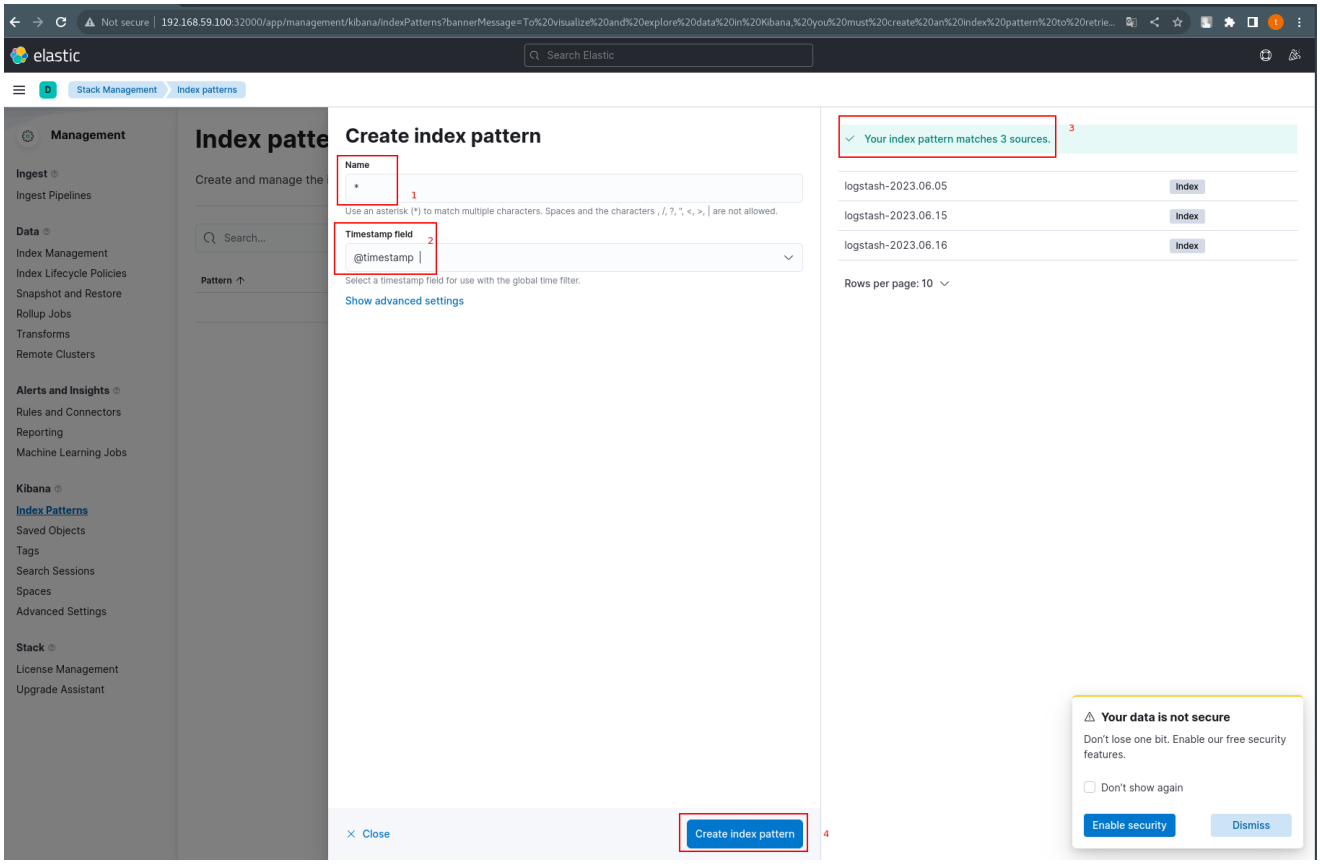
helm uninstall kibana -n logging-efk

4. Cấu hình Kibana UI

Mở trình duyệt web: http://192.168.59.100:32000/


Index patterns - Elastic
Not secure 192.168.59.100:32000/app/management/kibana/indexPatterns?bannerMessage=To%20visualize%20and%20explore%20data%20in%20Kibana,%20you%20must%20create%20an%20index%20pattern%20to%20
elastic
Search Elastic
Stack Management
Index patterns
1
Home
Analytics
Overview
Discover
2
Dashboard
Canvas
Maps
Machine Learning
Visualize Library
Enterprise Search
Overview
App Search
Workplace Search
Observability
Overview
Alerts
Cases
Logs
Metrics
Index patte
Create and manage the
Search...
Pattern
You have data in Elasticsearch.
Now, create an index pattern.
Kibana requires an index pattern to identify which data streams, indices, and index aliases you want to explore. An index pattern can point to a specific index, for example, your log data from yesterday, or all indices that contain your log data.
Create index pattern
3
Want to learn more?
Read documentation


Not secure 192.168.59.100:32000/app/discover#/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-15m,to:now))&_a=(columns:!(),filters:!(),index:'40253400-0c24-11ee-ae07-99e61e1a0810',interval:auto,query...
elastic
Search Elastic
Discover
Options
New
Open
Share
Inspect
Save
1
Home
Analytics
2
Overview
Discover
3
Dashboard
Canvas
Maps
Machine Learning
Visualize Library
Enterprise Search
Overview
App Search
Workplace Search
Observability
Overview
Alerts
Cases
Logs
Metrics
63
KQL
7
Last 15 minutes
Show dates
6
Refresh
2,087 hits
Chart options
4
100
80
60
40
20
0
15:46:00
15:47:00
15:48:00
15:49:00
15:50:00
15:51:00
15:52:00
15:53:00
15:54:00
15:55:00
15:56:00
15:57:00
15:58:00
15:59:00
16:00:00
Jun 16, 2023 @ 15:45:41.828 - Jun 16, 2023 @ 16:00:41.828
Time
Document
5
Jun 16, 2023 @ 16:00:33.000
@timestamp: Jun 16, 2023 @ 16:00:33.000 docker.container_id: 35a97c6dcc4530594f71d9b763c851056044b1e3c1410dd01f50f8be74b7df6c
kubernetes.container_image: docker.elastic.co/kibana/kibana:7.17.3 kubernetes.container_image_id: docker-
pullable://docker.elastic.co/kibana/kibana@sha256:9dd46102f9eadf43f62216a3113ed8b9ad675fe36706ff9daea8652f05d1a61e kubernetes.container_name: kibana
kubernetes.host: minikube kubernetes.labels.app: kibana kubernetes.labels.pod-template-hash: 68b94765bf kubernetes.labels.release: kibana
kubernetes.master_url: https://10.96.0.1:443/api kubernetes.namespace_id: 3e0b124b-d9b6-4b5c-9247-86f7bb60ff08
Jun 16, 2023 @ 16:00:32.000
@timestamp: Jun 16, 2023 @ 16:00:32.000 docker.container_id: 35a97c6dcc4530594f71d9b763c851056044b1e3c1410dd01f50f8be74b7df6c
kubernetes.container_image: docker.elastic.co/kibana/kibana:7.17.3 kubernetes.container_image_id: docker-
pullable://docker.elastic.co/kibana/kibana@sha256:9dd46102f9eadf43f62216a3113ed8b9ad675fe36706ff9daea8652f05d1a61e kubernetes.container_name: kibana
kubernetes.host: minikube kubernetes.labels.app: kibana kubernetes.labels.pod-template-hash: 68b94765bf kubernetes.labels.release: kibana
kubernetes.master_url: https://10.96.0.1:443/api kubernetes.namespace_id: 3e0b124b-d9b6-4b5c-9247-86f7bb60ff08
Jun 16, 2023 @ 16:00:32.000
@timestamp: Jun 16, 2023 @ 16:00:32.000 docker.container_id: 35a97c6dcc4530594f71d9b763c851056044b1e3c1410dd01f50f8be74b7df6c
kubernetes.container_image: docker.elastic.co/kibana/kibana:7.17.3 kubernetes.container_image_id: docker-
pullable://docker.elastic.co/kibana/kibana@sha256:9dd46102f9eadf43f62216a3113ed8b9ad675fe36706ff9daea8652f05d1a61e kubernetes.container_name: kibana
kubernetes.host: minikube kubernetes.labels.app: kibana kubernetes.labels.pod-template-hash: 68b94765bf kubernetes.labels.release: kibana



5. Gỡ cài đặt EFK

helm uninstall kibana -n logging-efk

helm uninstall elasticsearch -n logging-efk

helm uninstall fluentd -n logging-efk

kubectl ls pvc –n logging-efk

kubectl delete pvc elasticsearch-master-elasticsearch-master-0 -n logging-efk